# CA Process Automation

## Guida per l'amministratore del contenuto

Release 04.2.00

# Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA Catalyst per CA Service Desk Manager (connettore di CA Catalyst per CA SDM)
- CA Client Automation (precedentemente noto come CA IT Client Manager)
- CA Configuration Automation (precedentemente noto come CA Cohesion® Application Configuration Manager)
- CA CMBD (Database di gestione della configurazione di CA, CA Configuration Management Database)
- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA Infrastructure Insight (precedentemente noto come: CA Spectrum IM e CA NetQoS Reporter Analyzer combinati)
- CA NSM
- CA Process Automation (precedentemente noto come CA IT Process Automation Manager)
- CA Unicenter Service Catalog
- CA Service Desk Manager (CA SDM)
- CA Service Operations Insight (CA SOI) (precedentemente noto come CA Spectrum® Service Assurance)
- CA SiteMinder®
- CA Workload Automation AE

# Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

# Modifiche apportate alla documentazione

I seguenti aggiornamenti sono stati apportati alla documentazione nel tempo trascorso dall'ultimo rilascio della documentazione:

- Introduzione di CA Process Automation a nuovi utenti (a pagina 59): questo argomento esistente è stato aggiornato per includere la nuova *Guida di riferimento all'interfaccia utente*, che contiene le descrizioni dei campi.
- Esempio: Una singola Active Directory in due Active Directory di riferimento (a pagina 64): questo nuovo argomento offre un esempio che riguarda come CA EEM fa riferimento agli utenti di CA Process Automation con più Microsoft Active Directory, in cui lo stesso utente è definito per più Active Directory di riferimento.
- Configurazione delle impostazioni di protezione di CA EEM per il dominio (a pagina 140): questo argomento esistente è stato aggiornato per includere il valore del campo Dominio Active Directory predefinito, valido solo se CA EEM è configurato per l'utilizzo di più domini di Microsoft Active Directory.
- Configurazione delle proprietà di dominio (a pagina 147): questo argomento esistente è stato aggiornato per includere i nuovi campi relativi alla configurazione di gruppo host e all'eliminazione dei dati di reporting. Altri argomenti aggiornati allo stesso modo per la configurazione di gruppo host:
  - Configurazione delle proprietà dell'ambiente (a pagina 159)
  - Configurazione delle proprietà Touchpoint dell'orchestrator (a pagina 176)
  - Configurazione delle proprietà di host dell'orchestrator (a pagina 183)
  - Procedura per garantire un'elaborazione efficiente dei riferimenti del gruppo host (a pagina 267)
- Installazione interattiva di un agente (a pagina 204): questo argomento esistente è stato aggiornato per documentare una nuova casella di controllo che specifica se l'agente deve utilizzare la comunicazione semplificata (con NGINX o F5) o la comunicazione obsoleta (con Apache o F5). Viene precisato inoltre che Windows supporta le versioni jre7 e jre6. Altri argomenti aggiornati per tenere conto dei nuovi metodi di comunicazione:
  - Configurazione di proprietà dell'agente (a pagina 209)
  - Informazioni sulla comunicazione degli agenti (a pagina 221)
  - Configurazione degli agenti per l'utilizzo della comunicazione semplificata (a pagina 221)
  - Configurazione degli agenti per l'utilizzo della comunicazione obsoleta (a pagina 222)

- Scenario: Configurazione di touchpoint per la progettazione e la produzione (a pagina 225): questo nuovo scenario raccoglie le informazioni esistenti per mostrare la differenza delle opzioni di configurazione utilizzate in un ambiente di produzione da quelle utilizzate in un ambiente di progettazione.
- Casi in cui evitare l'utilizzo dei riferimenti di gruppo host come destinazioni (a pagina 268): questo argomento nuovo descrive l'impatto di un indirizzo IP specificato come destinazione di operatore per un processo da distribuire su un ambiente o dominio in cui la destinazione è un host diverso. Non è possibile modificare i processi esportati e importati come pacchetto di contenuto.
- Configurazione delle categorie operatore (a pagina 276): tutti gli argomenti compresi in questa sezione esistente sono stati riformulati per rimuovere le descrizioni dei campi aggiunte alla *Guida di riferimento all'interfaccia utente*.
- Pianificazione della struttura di cartella (a pagina 356): questo argomento esistente è stato riscritto per contemplare i requisiti per l'esportazione di una cartella come pacchetto di contenuto. Per questo nuovo metodo di esportazione è necessario che tutti gli oggetti di una versione di rilascio risiedano nella stessa cartella.
- Preparazione dell'ambiente di produzione per un nuovo rilascio (a pagina 370): questo processo esistente è stato riscritto per documentare la nuova opzione di esportazione della cartella come pacchetto di contenuto, che ha sostituito l'esportazione di un oggetto di automazione del pacchetto. Gli argomenti correlati comprendono quanto segue:
  - Informazioni sull'esportazione e sull'importazione di un pacchetto di contenuto (a pagina 371)
  - Scenario: Esportazione e importazione degli oggetti in un pacchetto di contenuto (a pagina 372): questo scenario include un esempio e le procedure e i concetti correlati.
- Eliminazione definitiva di oggetti e cartelle (a pagina 390): questo argomento esistente è stato aggiornato per documentare le conseguenze derivate dall'eliminazione di oggetti estratti. Si tratta di una nuova azione supportata in CA Process Automation r4.2.

# Sommario

## Capitolo 4: Gestione della protezione avanzata di CA EEM 73

## Capitolo 5: Amministrazione del dominio di CA Process Automation 137



## Capitolo 6: Amministrazione degli ambienti 157



## Capitolo 7: Amministrazione di orchestrator 171

## Capitolo 13: Amministrazione di trigger 323



## Capitolo 14: Gestisci risorse utente 337



## Capitolo 15: Controllo delle azioni dell'utente 345



## Capitolo 16: Amministrazione degli oggetti di libreria 355

# Capitolo 1: Guida introduttiva

Quando si installa inizialmente CA Process Automation con CA EEM configurato con un archivio utenti interno, CA Process Automation presenta un utente amministratore predefinito con le credenziali seguenti:

**Nome utente**

pamadmin

**Password**

pamadmin

È possibile accedere a un'istanza del prodotto appena installato ed effettuare l'accesso con queste credenziali. Un metodo più efficace consiste nel creare un account utente in CA EEM durante la prima sessione, quindi accedere a CA Process Automation con le credenziali definite.

Dopo aver effettuato l'accesso, configurare le impostazioni con cui amministrare la protezione e configurare il dominio.

Questa sezione contiene i seguenti argomenti:

# Accedere a CA EEM come utente EiamAdmin.

L'utente EiamAdmin può accedere a CA EEM e gestire le identità (account utente) e le policy di accesso.

**Attenersi alla procedura seguente:**

1. Accedere all'URL per l'istanza di CA EEM utilizzata da CA Process Automation:

   `https://`*`hostname`*`:5250/spin/eiam`

   ***nome host***

   Definisce il nome host o l'indirizzo IP del server in cui CA EEM è installato.

   **Nota:** Per determinare il nome host di CA EEM utilizzato da CA Process Automation, controllare il campo Server di backend CA EEM nella scheda Configurazione di CA Process Automation, sottoscheda Protezione.

2. Dall'elenco a discesa Applicazione, selezionare il valore configurato per Nome applicazione EEM durante l'installazione.

   **Nota:** Questo è il nome con cui CA Process Automation è stato registrato con CA EEM.

3. Digitare **EiamAdmin** e la password definita per l'utente EiamAdmin.
4. Fare clic su Accedi.

# Creazione del primo Account di amministratore

È possibile creare il proprio account utente di CA Process Automation in CA EEM e concedere l'accesso completo (Amministratore) a CA Process Automation.

**Attenersi alla procedura seguente:**

1. Accedere a CA EEM come utente EiamAdmin. (a pagina 16)
2. Fare clic sulla scheda Gestisci identità.
3. Fare clic sull'icona accanto a Utenti nel relativo riquadro.

   Viene visualizzata la pagina Nuovo utente.

4. Nel campo Nome digitare l'ID utente che si desidera inserire come nome utente quando si accede a CA Process Automation.
5. Fare clic su Aggiungi informazioni su utente applicazione.

6. Selezionare il gruppo PAMAdmins dai gruppi di utenti disponibili e fare clic su > per spostarlo nei gruppi di utenti selezionati.

   Il gruppo concede l'accesso completo a tutte le funzioni in CA Process Automation.

7. Immettere i propri dettagli nella sezione relativa ai dettagli dell'utente globale del profilo dell'account utente.

8. (Facoltativo) Completare il campo Appartenenza gruppo globale se si utilizza CA Process Automation con un altro prodotto di CA Technologies che utilizza CA EEM.

9. Nell'area Autenticazione creare la password che si desidera inserire quando si accede a CA Process Automation.

10. (Facoltativo) Completare i campi restanti nella pagina Nuovo utente.

11. Fare clic su Salva.

    Un messaggio di conferma indica: Informazioni su utente globale create correttamente. Informazioni su utente applicazione create correttamente.

12. Fare clic su Chiudi.

13. Fare clic su Disconnetti.

**Ulteriori informazioni:**

Utilizzo di CA EEM per la modifica della password di CA Process Automation (a pagina 46)
Concessione dell'accesso a CA EEM ad amministratori specifici (a pagina 75)

# Accesso a CA Process Automation

L'URL utilizzato per accedere a CA Process Automation varia se l'orchestrator di dominio viene configurato con un nodo (non cluster) o con più nodi (in cluster). È possibile accedere direttamente a un CA Process Automation non cluster. Per un CA Process Automation in cluster, accedere all'utilità di bilanciamento del carico associata. È possibile raggiungere tutti gli orchestrator nel dominio avviando l'URL all'orchestrator di dominio o all'utilità di bilanciamento del carico per l'orchestrator di dominio.

**Attenersi alla procedura seguente:**

1. Accedere a CA Process Automation.

   - Per comunicazioni protette, utilizzare la seguente sintassi:
     `https://`*`server`*`:`*`port`*`/itpam`

     **Esempi:**
     ```
     https://Orchestrator_host:8443/itpam
     https://loadBalancer_host:443/itpam
     ```

   - Per comunicazioni di base, utilizzare la seguente sintassi:
     `http://`*`server`*`:`*`port`*`/itpam`

     **Esempi:**
     ```
     http://Orchestrator_host:8080/itpam
     http://loadBalancer_host:80/itpam
     ```

   Viene visualizzata la pagina di accesso a CA Process Automation.

2. Immettere le credenziali dal proprio account utente.

   **Nota:** Se CA EEM è configurato per fare riferimento agli utenti di più Microsoft Active Directory e CA Process Automation non accetta il nome utente non completo, immettere il proprio nome principale, ovvero *domain_name**user_name*.

3. Fare clic su Accedi.

   L'applicazione CA Process Automation si apre. Viene visualizzata la scheda Pagina iniziale.

# Impostazione della lingua e dei formati di data e ora

Per impostazione predefinita, la data e l'ora relative all'orchestrator di dominio vengono visualizzate nel fuso orario del browser. Durante la prima sessione di accesso, è possibile impostare i formati di data e ora nonché la lingua di preferenza.

**Nota:** Il prodotto archivia le date e le ore in Coordinated Universal Time (UTC).

**Attenersi alla procedura seguente:**

1. Andare a CA Process Automation ed eseguire l'accesso (a pagina 18), se non ancora eseguito.
2. Nella barra degli strumenti, fare clic sul proprio nome utente.
3. Nella finestra di dialogo Impostazioni utente, selezionare i formati preferiti per data e ora.
4. Verificare e modificare l'impostazione della lingua, se necessario.
5. Fare clic su Salva e chiudi.
6. Fare clic su OK.
7. Fare clic su Disconnetti.

   Le impostazioni diventano effettive quando si esegue nuovamente l'accesso.

# Aggiornamento del contenuto predefinito

Nuovo contenuto predefinito è disponibile periodicamente. Solo un amministratore può importare il nuovo contenuto predefinito. Per garantire che la cartella PAM_PreDefinedContent includa l'ultimo contenuto predefinito, ripetere occasionalmente la procedura di aggiornamento.

**Attenersi alla procedura seguente:**

1. Eliminare il contenuto importato in precedenza.
   a. Fare clic sulla scheda Libreria.
   b. Selezionare la cartella PAM_PreDefinedContent, fare clic su Elimina, quindi fare clic su Sì nel messaggio di conferma.

      La cartella PAM_PreDefinedContent viene spostata nel cestino. (Comprimere la struttura della cartella per visualizzare il cestino.)
   c. Selezionare la cartella PAM_PreDefinedContent nel cestino, quindi fare clic su Elimina.
2. Fare clic sulla scheda Pagina iniziale.

3. Fare clic su Sfoglia contenuto predefinito.
4. Fare clic su Sì per confermare l'importazione.

   Il processo di importazione crea la cartella PAM_PreDefinedContent con il contenuto più recente nella directory principale della scheda Libreria.

# Controllo dell'intervallo di timeout

È possibile modificare l'intervallo di timeout del prodotto. Per impostazione predefinita, il prodotto si disattiva automaticamente dopo 15 minuti di inattività.

**Attenersi alla procedura seguente:**

1. Accedere come amministratore al server in cui l'orchestrator di domino è installato.
2. Accedere alla seguente cartella:

   `install_dir/server/c2o/.config`

   ***install_dir***

   Definisce l'host in cui è installato l'orchestrator di dominio.
3. Aprire il file OasisConfig.properties con un editor.
4. Utilizzare Trova per localizzare la proprietà seguente:

   `managementconsole.timeout`
5. Modificare il valore della proprietà.
6. Salvare il file e uscire.
7. Riavviare il servizio dell'orchestrator.
   a. Interrompere l'orchestrator (a pagina 196).
   b. Avviare l'orchestrator (a pagina 197).

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

# Impostazioni consigliate del browser Internet Explorer per l'autenticazione pass-through NTLM

Le impostazioni consigliate per il browser Internet Explorer (IE) di Windows per l'autenticazione pass-through NTLM si applicano nei casi seguenti (se CA EEM punta a servizi Active Directory esterni):

- CA EEM utilizza l'autenticazione pass-through NTLM per autenticare utenti globali di CA Process Automation.
- Gli utenti utilizzano Internet Explorer per accedere a CA Process Automation.
- Internet Explorer richiede l'inserimento di nome utente e password.

**Attenersi alla procedura seguente:**

1. Dal menu Strumenti di Internet Explorer, selezionare Opzioni Internet, quindi fare clic sulla scheda Protezione.
2. Selezionare l'icona Intranet locale, quindi fare clic su Livello personalizzato.

   Viene visualizzata la finestra di dialogo Impostazioni di protezione - Area Intranet locale.
3. Scorrere fino alla voce Autenticazione utente e selezionare Accesso automatico solo nell'area Intranet.
4. Aggiungere l'URL di CA Process Automation all'Area Intranet locale.

# Informazioni sulla Guida

La *Guida per l'amministratore del contenuto* tratta le attività eseguite dagli utenti con i seguenti ruoli:

- CA EEM Amministratori che eseguono la configurazione CA EEM per CA Process Automation.
- Amministratori del contenuto di CA Process Automation con diritti di amministratore di dominio, amministratore della configurazione di ambiente e amministratore del contenuto di ambiente.

Le attività dell'amministratore del contenuto includono:

- Impostazione della protezione.
- Configurazione del prodotto per il supporto dello sviluppo dei contenuti e della produzione.

Prima di iniziare a utilizzare questa guida, assicurarsi che le attività di installazione e configurazione descritte nella *Guida all'installazione* di CA Process Automation siano state completate.

**Note:**

- Per i flussi di lavoro relativi alla configurazione di un nuovo ambiente di progettazione dei contenuti o un nuovo ambiente di produzione, consultare la *Guida in linea*.
- Per informazioni sull'utilizzo dei metodi di servizio Web da parte dei responsabili di progettazione dei contenuti, consultare la *Guida di riferimento per le API dei servizi Web*.
- Per informazioni sul modo in cui i responsabili di progettazione dei contenuti creano i processi e altri oggetti di automazione, consultare la *Guida alla progettazione dei contenuti*.
- Per informazioni sugli operatori, consultare la *Guida di riferimento per la progettazione dei contenuti*.
- Per informazioni sul modo in cui gli utenti dell'ambiente di produzione utilizzano il prodotto in un ambiente di produzione, consultare la *Guida per l'utente dell'ambiente di produzione*.
- Per informazioni sul modo in cui i responsabili di progettazione utilizzano la scheda Operazioni durante la progettazione dei contenuti, consultare la *Guida per l'utente dell'ambiente di produzione*.

# Capitolo 2: Panoramica per amministratori

Questa sezione contiene i seguenti argomenti:



## Panoramica delle attività di amministrazione

L'interfaccia principale di CA Process Automation consente lo sviluppo dei contenuti. Gli amministratori di sistema e gli amministratori del contenuto utilizzano CA Process Automation per le attività seguenti:

- Amministrazione di protezione.

  La protezione per CA Process Automation implica l'autenticazione dell'utente durante il login e l'accesso in base ai ruoli. Si definiscono account utente, gruppi personalizzati e norme che concedono autorizzazioni in CA EEM.

- Amministrazione del dominio.

  *Dominio* è il termine utilizzato per descrivere la visualizzazione a livello aziendale dell'intero sistema CA Process Automation, inclusi orchestrator, agenti e librerie di processo. L'amministrazione di dominio include l'aggiunta di ambienti, la rimozione di agenti inutilizzati e di touchpoint in blocco, e la gestione di proprietà di dominio.

- Configurazione degli orchestrator.

  Un *orchestrator* è il componente del modulo CA Process Automation che esegue la lettura dalla libreria di processo e i processi. Il primo orchestrator di CA Process Automation che viene installato è l'orchestrator di dominio. È possibile aggiungere altri nodi all'orchestrator di dominio per ottenere una potenza di elaborazione e un bilanciamento del carico maggiori. Se gli utenti si trovano in località diverse, valutare l'aggiunta di un nuovo orchestrator standard in ciascuna posizione.

- Creazione e configurazione di ambienti.

  Un *ambiente* è una partizione facoltativa del dominio che separa lo sviluppo di contenuti. È possibile creare ambienti per attività di sviluppo, test e produzione, oppure per unità di business differenti. La configurazione include l'aggiunta di touchpoint e la creazione di gruppi touchpoint.

- Configurazione degli agenti.

  Un *agente* è un'applicazione software di CA Process Automation installata su un host di rete. Gli orchestrator che eseguono processi possono effettuare alcune operazioni del processo sugli host agente o remoti con connessione SSH agli gli. La configurazione comprende l'associazione di touchpoint, touchpoint proxy o gruppi host agli agenti.

- Mapping e configurazione dei touchpoint.

  Un *touchpoint* è un'entità logica utilizzata nelle definizioni dell'operatore per rappresentare l'agente o l'orchestrator di destinazione in cui eseguire una porzione del processo. È possibile mappare un touchpoint su molti agenti simultaneamente e su agenti differenti in momenti successivi. I touchpoint offrono flessibilità nell'implementazione dei processi, riducendo al tempo stesso i requisiti di manutenzione dei processi stessi.

- Mapping e configurazione di touchpoint proxy e gruppi host.

  Gli host remoti, ossia gli host senza un agente installato, possono essere utilizzati come destinazione per l'esecuzione di operazioni come parte di un processo in esecuzione. Per abilitare la connettività, stabilire l'accesso SSH da un host con un agente all'host remoto. Configurare un touchpoint proxy o un gruppo host sull'host con agente. Un operatore può impostare come destinazione un host utilizzandone il nome del touchpoint proxy. Un gruppo host fa riferimento a host remoti. Un operatore può impostare come destinazione tale host remoto utilizzandone l'FQDN o l'indirizzo IP.

  **Nota:** consultare la sezione Sintassi per nomi host DNS (a pagina 407).

- Esplorazione della libreria.

  Una *libreria* è il repository contenente script e oggetti operatore che i responsabili di progettazione dei contenuti assemblano per la creazione di processi. I processi e gli altri oggetti di automazione vengono archiviati nella libreria.

- Amministrazione degli oggetti di automazione nelle librerie.

  Gli *oggetti di automazione* permettono di definire l'elaborazione, la pianificazione, il monitoraggio, la registrazione e altri elementi configurabili di un pacchetto CA Process Automation. Gli oggetti di automazione vengono memorizzati in una libreria di un orchestrator specifico in un'architettura non cluster. L'amministrazione degli oggetti di automazione comprende la configurazione facoltativa delle impostazioni di protezione in un oggetto o cartella di libreria per il controllo dell'accesso di gruppi e utenti designati.

- Gestione della protezione per oggetti di automazione.

  È possibile creare norme di CA EEM personalizzate per oggetti di automazione. Ad esempio, abilitare Protezione touchpoint e creare norme di Protezione touchpoint in CA EEM per limitare chi può eseguire determinati operatori su destinazioni specificate di grande importanza. Abilitare Protezione runtime e utilizzare Imposta titolare per concedere diritti di avvio del processo solo al titolare del processo.

- Amministrazione dei processi.

  Un esempio di amministrazione di processi è l'interruzione dei processi non riusciti da una visualizzazione processo.

# Panoramica delle schede

La disponibilità di schede specifiche nell'interfaccia utente del prodotto dipende dai diritti di accesso concessi all'utente connesso. Quando si accede al prodotto per la prima volta, l'interfaccia utente visualizza le schede descritte da questo argomento.

**Nota:** La maggior parte delle attività di configurazione e amministrazione viene eseguita dalla scheda Configurazione. Per flussi di attività relativi a ciascuna scheda, consultare la *Guida in Linea*.

**Pagina iniziale**

La scheda Pagina iniziale consente un rapido accesso agli oggetti in uso. È possibile utilizzare altri collegamenti per eseguire velocemente l'accesso a informazioni di interesse generale.

**Libreria**

In genere, gli amministratori del contenuto creano le cartelle e assegnano i relativi diritti di accesso.

**Nota**: I responsabili di progettazione dei contenuti creano gli oggetti e accedono ad essi per modificare dalle cartelle della scheda Libreria. La scheda Progettazione è l'editor per oggetti di processo.

**Cartelle**

In genere, un amministratore imposta una struttura delle cartelle nell'ambiente di progettazione. Le cartelle contengono cartelle secondarie e oggetti di automazione. Come procedura consigliata, creare una cartella per ogni processo da automatizzare, con una cartella secondaria per ciascuna versione di rilascio di quel processo. Le cartelle a livello di processo possono essere a livello principale.

La cartella che contiene la versione di rilascio di un processo viene esportata come pacchetto di contenuto e poi importata nell'ambiente di produzione. Il processo di importazione duplica la struttura delle cartelle nell'ambiente di produzione. Tuttavia, la libreria di produzione contiene solo la versione di rilascio del processo e gli oggetti correlati. Le cartelle non vengono create manualmente nella libreria di produzione.

**Cestino**

Il Cestino nella parte inferiore del nodo Orchestrator contiene cartelle e oggetti che sono stati eliminati. Quando si fa clic su Cestino, è possibile selezionare cartelle e oggetti eliminati da eliminare in modo definitivo dalla libreria o da ripristinare nella libreria.

**Cerca**

Definire i criteri per cartella, parola chiave o dati in base ai quali cercare gli oggetti di contenuto nel campo Cerca.

**Sommario**

I responsabili di progettazione dei contenuti creano le istanze di oggetti di automazione selezionati in una cartella. Aprono le istanze create dalla porzione dei contenuti della scheda Libreria.

**Progettazione**

I responsabili di progettazione dei contenuti progettano un processo pianificato nella scheda Progettazione.

**Operazioni**

La scheda Operazioni viene utilizzata dagli utenti nel gruppo degli utenti dell'ambiente di produzione.  include i seguenti riquadri:

**Collegamenti**

Visualizza informazioni nel riquadro destro per i seguenti collegamenti standard:

**Istanze di processo**

Istanze dei processi avviati. Il grafico a barre nel riquadro Istanze di processo visualizza gli operatori in base allo stato. Il riquadro Istanze di processo visualizza anche i dettagli per ciascun operatore.

**Operatori**

Operatori in attività e processi avviati da pianificazioni. Il grafico a barre nel riquadro Operatori visualizza gli operatori in base allo stato. Il riquadro Operatori visualizza anche i dettagli per ciascun operatore.

**Attività**

Attività che sono assegnate a utenti e gruppi. Tutti gli utenti possono visualizzare l'elenco di attività specifiche e gli elenchi di attività per i gruppi di appartenenza, nonché le attività assegnate ad altri utenti. Gli amministratori assegnano attività a utenti o a gruppi. Un utente svolge un'attività assegnata e risponde alla notifica Interazione utente.

**Pianificazioni attive**

Pianificazioni che hanno avviato i processi attivi.

**Pianificazioni globali**

Pianificazioni che ogni utente può utilizzare per avviare un processo o gli operatori selezionati. È possibile filtrare la visualizzazione in base a data, orchestrator o touchpoint agente, nonché in base allo stato della pianificazione, ovvero corrente o archiviato.

**Richieste di avvio**

Richiede di avviare i processi specificati su richiesta.

**Pacchetti di contenuto**

Tutti gli utenti possono controllare gli oggetti importati nell'ambiente come pacchetti di contenuto. Quando si fa clic su un pacchetto di contenuto nel riquadro sinistro, le proprietà del pacchetto vengono visualizzate nel riquadro destro.

**Nota**: È possibile visualizzare le informazioni sulla versione di rilascio per gli elementi seguenti che sono inclusi in pacchetti di contenuto:

- Istanze di processo
- Pianificazioni attive
- Pianificazioni globali
- Richieste di avvio

Il prodotto visualizza il nome del pacchetto di contenuto e la versione di rilascio del pacchetto di contenuto per ciascun oggetto.

**Visualizzazione processo**

Tutti gli utenti possono monitorare i processi in tutti gli stati, pianificazioni attive, operatori, richieste di inizio, set di dati, risorse e operatori personalizzati.

**Richieste di avvio**

Gli utenti possono visualizzare un grafico a barre delle istanze di richiesta di avvio con stato in coda, in esecuzione, completato e non riuscito. Per una barra selezionata, gli utenti possono visualizzare il nome di istanza, il tempo pianificato, lo stato, l'ora di inizio e l'ora di fine, e il nome utente.

**Set di dati**

Gli utenti possono visualizzare la struttura di un set di dati selezionato e le relative coppie nome/valore.

**Risorse**

Gli utenti possono selezionare un oggetto risorse, quindi utilizzare il riquadro destro per sostituire manualmente i valori Quantità e Utilizzato. Gli utenti possono modificare anche lo Stato.

**Pianificazioni**

Gli utenti possono selezionare una pianificazione, quindi utilizzare il riquadro destro per impostare le proprietà seguenti:

- La data di esecuzione
- Se visualizzare l'attività per tutti i nodi o per un orchestrator selezionato
- Se visualizzare le pianificazioni archiviate

**Configurazione**

L'amministratore è responsabile della configurazione dell'accesso a CA Process Automation nella scheda Configurazione. Per impostazione predefinita, ambienti, orchestrator e agenti ereditano le impostazioni che gli amministratori configurano a livello di dominio. Gli operatori ereditano le impostazioni che gli amministratori configurano a livello di categoria di operatore. La scheda Configurazione contiene i seguenti riquadri:

**Browser di configurazione**

Visualizza i nodi seguenti:

**Dominio**

Consente di configurare il dominio, l'ambiente predefinito, il touchpoint dell'orchestrator, i touchpoint dell'agente, i touchpoint proxy e i gruppi host.

**Orchestrator**

Consente di configurare l'orchestrator di dominio e altri orchestrator installati.

**Agenti**

Consente di configurare le associazioni e le impostazioni per tutti gli agenti installati.

**Gestisci risorse utente**

L'amministratore di sistema accede alla cartella Risorse utente per aggiungere o aggiornare gli script utilizzati per lo sviluppo dei contenuti. Gli amministratori possono caricare file JAR nella cartella Risorse agente o Risorse orchestrator. Il prodotto condivide i file caricati quando si riavviano gli agenti o gli orchestrator.

**Installazioni**

L'amministratore di sistema installa altri orchestrator o nodi cluster per l'orchestrator di dominio o altri orchestrator. Gli amministratori installano anche agenti.

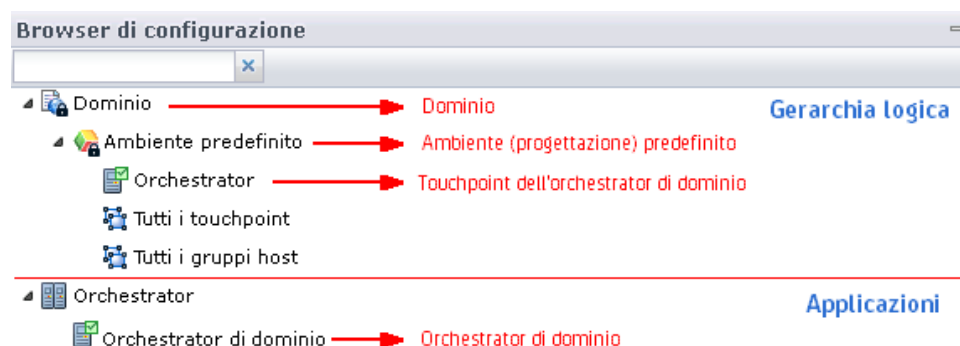
**Report**

Tutti gli utenti possono accedere ai report predefiniti o caricare i report personalizzati progettati con la progettazione BIRT RCP.

# Relazioni tra i componenti

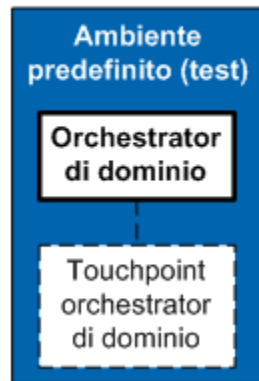
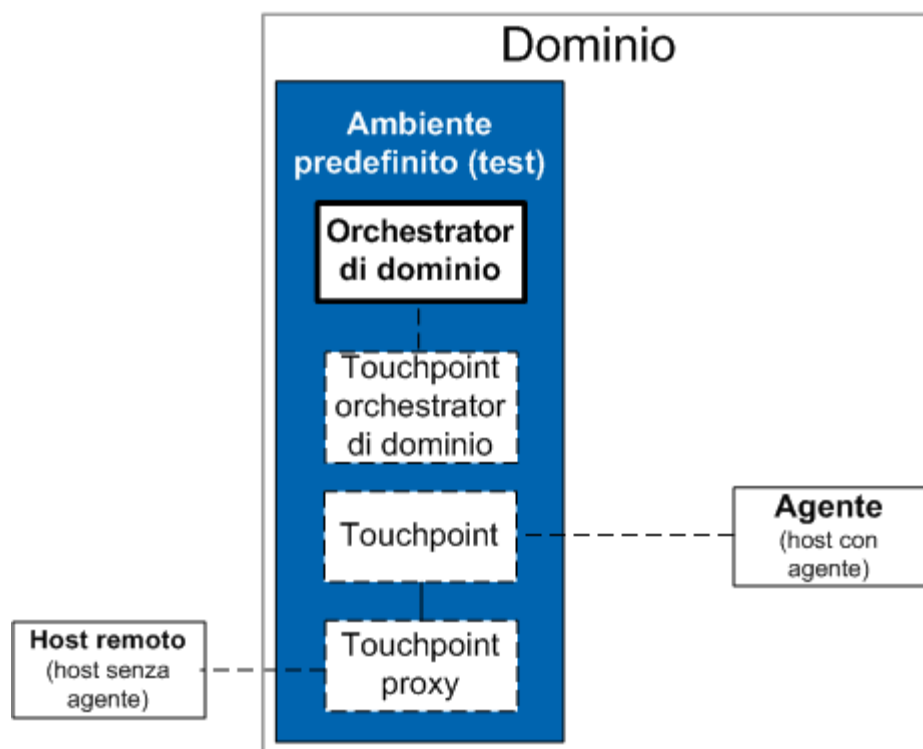
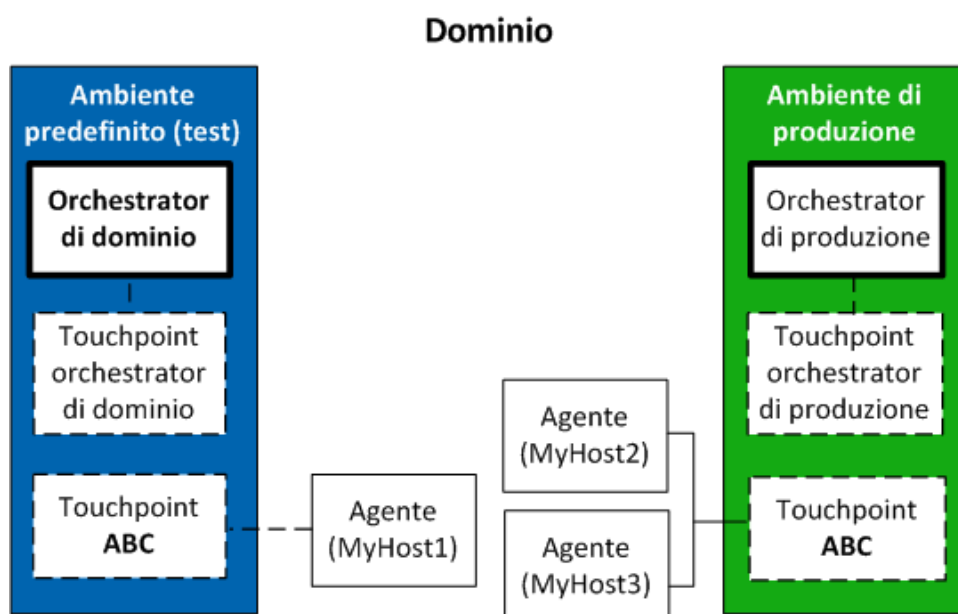
Le responsabilità di un amministratore di CA Process Automation includono:

- Configurazione: dominio, ambiente predefinito o orchestrator
- Installazione e configurazione per la costruzione del dominio: altri orchestrator e agenti.
- Creazione e configurazione delle entità logiche: ambienti, touchpoint (inclusi i touchpoint proxy) e gruppi host.

Prima di continuare, è utile comprendere le relazioni tra queste entità logiche e fisiche. Il riquadro Browser di configurazione nella scheda Configurazione visualizza una struttura della gerarchia logica, il nodo Orchestrator e il nodo Agenti vuoto. La gerarchia logica è costituita inizialmente dal nodo Dominio con il nodo Ambiente predefinito. Il nodo Ambiente predefinito espanso visualizza l'orchestrator, il nodo Tutti i touchpoint vuoto e il nodo Tutti i gruppi host vuoto.

Il dominio è il nodo principale nella gerarchia logica. Tutti gli orchestrator installati vengono visualizzati sotto il nodo Orchestrator. Tutti gli agenti installati vengono visualizzati sotto il nodo Agenti (non mostrato nella figura).

Il termine touchpoint fa riferimento all'associazione tra un orchestrator e un ambiente. Inoltre, un touchpoint fa anche riferimento all'associazione tra un agente e un ambiente. L'illustrazione mostra il browser di configurazione come viene visualizzato subito dopo la prima installazione di CA Process Automation. Pertanto non include agenti o touchpoint agente. I responsabili di progettazione dei contenuti utilizzano i touchpoint come destinazioni all'interno dei processi che automatizzano. (L'uso e il vantaggio dei touchpoint vengono descritti in un'altra sezione.)

In genere l'ambiente Predefinito è dedicato alla progettazione di processi automatizzati. I responsabili di progettazione dei contenuti sviluppano il processo in esecuzione sul touchpoint dell'orchestrator di dominio. Quando il primo processo è pronto per passare alla produzione, creare un nuovo ambiente. In tal modo, un ambiente di produzione viene aggiunto al dominio.

Nell'illustrazione seguente il touchpoint è rappresentato come un blocco dai bordi tratteggiati. Nell'illustrazione l'associazione tra il touchpoint e l'orchestrator di dominio è rappresentata da una linea tratteggiata.

Un processo in esecuzione su un orchestrator può includere operatori che devono utilizzare come destinazione altri host. In genere tali destinazioni richiedono l'installazione di un agente di CA Process Automation, quindi l'associazione dei touchpoint all'agente. I responsabili di progettazione dei contenuti accedono all'agente attraverso il relativo nome di touchpoint. Quando non è possibile installare un agente su un host di destinazione, vengono usati i touchpoint proxy. Un *touchpoint proxy* estende l'uso dei touchpoint in modo che gli orchestrator possano eseguire gli operatori su un host remoto (ovvero su un host senza alcun agente installato). Quando un touchpoint è configurato con una connessione SSH tra l'host agente e un host remoto, si tratta di un touchpoint proxy.

Per ciascun touchpoint con un'associazione all'ambiente di progettazione, si aggiunge un touchpoint con lo stesso nome e lo si associa all'ambiente di produzione. Pertanto, un operatore in esecuzione sul touchpoint ABC nell'ambiente di progettazione viene eseguito anche su un touchpoint con lo stesso nome nell'ambiente di produzione. Nell'ambiente di test, è possibile associare il touchpoint a un solo agente. Per supportare l'alta disponibilità nell'ambiente di produzione, è possibile associare il touchpoint corrispondente a due agenti.

**Ulteriori informazioni:**

Informazioni su orchestrator, agenti e la gerarchia di dominio (a pagina 152)

# Cardinalità delle associazioni dei componenti

L'amministratore di CA Process Automation costruisce il dominio installando orchestrator e agenti. Esegue la partizione del dominio creando degli ambienti, tutti dotati della propria libreria. Configura i touchpoint per i responsabili di progettazione dei contenuti da specificare come destinazioni per gli operatori. Fare clic sulla scheda Configurazione e aprire il riquadro Browser di configurazione per visualizzare queste entità.

Le regole seguenti governano la cardinalità tra coppie di entità che possono avere un'associazione:

**Dominio, ambienti, orchestrator, agenti**

Gli orchestrator e gli agenti sono componenti software installati *fisicamente* sugli host. Il dominio e gli ambienti sono entità *logiche*.

- Un sistema di CA Process Automation dispone esclusivamente di un dominio.
- Quando viene installato un nuovo sistema di CA Process Automation, il dominio ha un ambiente predefinito. L'ambiente predefinito contiene l'orchestrator di dominio.
- Il dominio può avere molti ambienti. È possibile aggiungere ambienti a librerie separate. Ad esempio, è possibile dedicare l'ambiente predefinito alla progettazione e al test dei nuovi contenuti. In seguito, è possibile creare un ambiente distinto per la produzione. Ogni ambiente deve disporre almeno di un orchestrator.

  **Nota:** generalmente, un amministratore esporta i contenuti dall'ambiente predefinito e quindi li importa nell'ambiente di produzione. È anche possibile trasferire i contenuti tra i domini.

- Un ambiente può avere uno o più orchestrator. Ciascun orchestrator è installato su un host separato.

  **Nota:** un orchestrator può essere *standard* o *cluster*. Un orchestrator cluster comprende più nodi. Ciascun nodo è installato su un host separato. Un orchestrator sia in cluster sia standard (non cluster) viene visualizzato come un'entità singola nel riquadro Browser di configurazione.

- Il dominio può disporre di tutti gli agenti necessari. Gli agenti vengono installati su host e sono indipendenti dagli ambienti.

**Ambienti e touchpoint**

Gli ambienti e i touchpoint sono entità *logiche*.

- Ogni touchpoint appartiene a un solo ambiente.
- Ogni ambiente può avere più touchpoint.
- Per ciascun touchpoint utilizzato in una versione di rilascio di un processo nell'ambiente di progettazione, deve esistere un touchpoint denominato in maniera identica nell'ambiente di produzione. Ciò consente l'esecuzione del processo non modificabile nell'ambiente di produzione.

**Orchestrator e touchpoint**

Dopo avere installato un orchestrator, si crea un touchpoint per associare l'orchestrator a un ambiente specifico. Gli operatori in un processo utilizzano come destinazione il touchpoint associato all'orchestrator. L'associazione di touchpoint determina l'ambiente in cui il processo viene eseguito.

- L'orchestrator di dominio ha un touchpoint predefinito.
- Ogni orchestrator è associato a un solo touchpoint.
- Un touchpoint associato a un orchestrator non è mai associato a un agente. Le associazioni touchpoint-orchestrator e touchpoint-agente si escludono a vicenda.
- Un operatore viene eseguito sul touchpoint dell'orchestrator che esegue il processo se la destinazione dell'operatore è vuota.

### Agenti e touchpoint

Per rendere un agente disponibile come destinazione per un operatore, associare l'agente a un touchpoint, un touchpoint proxy o un gruppo host.

- È possibile associare un agente a uno o più touchpoint.
  - Quando si associa un agente a un touchpoint, è possibile eseguire gli operatori direttamente su un host con un agente installato utilizzando come destinazione il touchpoint.
  - Quando si associa un agente a più touchpoint sullo stesso host, i touchpoint in genere utilizzano come destinazione diversi componenti sull'host. Ad esempio, si potrebbe definire un touchpoint per l'accesso a un database e uno per l'accesso a un prodotto di terze parti.
  - Ciascun operatore in un processo viene eseguito su un touchpoint che può essere associato a un operatore, a un agente o a più agenti. Se operator-1 viene eseguito su Touchpoint-ABC nell'ambiente di progettazione, viene eseguito su un touchpoint diverso chiamato Touchpoint-ABC nell'ambiente di produzione. Ogni membro di questa coppia di touchpoint viene associato a un ambiente diverso. È possibile associare ciascun membro della coppia di touchpoint allo stesso agente oppure a diversi agenti. Questo tipo di associazione consente di definire processi di cui è possibile eseguire la migrazione da un ambiente all'altro senza modificare le informazioni sull'host di destinazione.
- È possibile associare un touchpoint a uno o più agenti. È possibile assegnare la stessa priorità a più agenti o una priorità diversa a ciascun agente.
  - Quando gli agenti hanno priorità differenti, gli operatori vengono eseguiti sull'agente con la priorità più alta. Se l'agente con priorità più alta non è disponibile, gli operatori vengono eseguiti su un agente disponibile con una priorità inferiore. Questo meccanismo permette di avere un host di destinazione sempre disponibile.
  - Quando più agenti con la stessa priorità vengono associati a un touchpoint, gli operatori vengono eseguiti su un agente selezionato a caso. Questa struttura promuove il bilanciamento del carico.
  - Un touchpoint associato a un orchestrator non è mai associato a un agente.

**Agenti, touchpoint proxy e host remoti**

Un host remoto fa riferimento a un host che è la destinazione di un operatore quando l'installazione di un agente non è fattibile.

- È possibile associare un agente a uno o più touchpoint proxy.
- Un *touchpoint proxy* è un touchpoint configurato con una connessione SSH a un host remoto. L'host remoto in genere non ha alcun agente.
- Quando si associa un agente a un touchpoint proxy, gli operatori in un processo possono utilizzare come destinazione il touchpoint proxy per l'esecuzione sull'host remoto.

**Nota:** Un orchestrator può distribuire il carico di lavoro a un host remoto senza utilizzare un agente mediante l'operatore Esegui script SSH in un processo. Il responsabile di progettazione dei contenuti definisce i parametri di configurazione (nell'operatore) che specificano l'indirizzo e le credenziali dell'host da utilizzare per la connessione SSH all'host remoto ed eseguire uno script. Per informazioni sull'operatore Esegui script SSH, consultare la *Guida di riferimento per la progettazione dei contenuti*.

**Agenti, gruppi host e host remoti**

Un *gruppo host* è un gruppo di host remoti. Generalmente si configurano i gruppi host con un modello di nome host comune o con una subnet IPv4 espressa nella notazione CIDR.

- È possibile associare un agente a uno o più gruppi host.
- È possibile associare un gruppo host a uno o più agenti.
- Quando un agente è associato a un gruppo host, le connessioni SSH si configurano manualmente. Configurare una connessione SSH dall'host agente per ciascun host remoto cui fa riferimento il gruppo host.
- Quando un agente è associato a un gruppo host, gli operatori all'interno di un processo sono eseguiti su un host remoto di riferimento. Gli operatori usano come destinazione l'indirizzo IP o il nome di dominio completo (FQDN) dell'host remoto.

**Nota:** Per la comunicazione SSH non interattiva con un host remoto, utilizzare un touchpoint proxy o un gruppo host. Per la comunicazione SSH interattiva con un host remoto, utilizzare l'operatore Esegui script SSH. Per informazioni sull'operatore Esegui script SSH, consultare la *Guida di riferimento per la progettazione dei contenuti*.

# Protezione

Ai fini della protezione di CA Process Automation, l'amministratore deve occuparsi di quanto segue:

- Proteggere l'applicazione CA Process Automation (a pagina 39).
- Sospendere o disabilitare un account utente (a pagina 40).
- Proteggere il trasferimento di dati con crittografie forti (a pagina 41).
- Proteggere il trasferimento di dati tra CA Process Automation e CA EEM (a pagina 41).

**Ulteriori informazioni:**

Amministrazione della protezione di base di CA EEM (a pagina 43)

## Proteggere l'applicazione CA Process Automation

Una misura di protezione dell'applicazione consiste nell'impedire l'accesso agli utenti non autorizzati. Un'altra consiste nel limitarne l'utilizzo in base al ruolo dell'utente che ha eseguito l'accesso. La protezione dell'applicazione include i meccanismi seguenti:

**Autenticazione**

Il prodotto utilizza CA EEM per l'autenticazione degli utenti all'accesso. CA EEM confronta le credenziali immesse dagli utenti all'accesso con le combinazioni di nome utente e password negli account utente. L'utente può accedere solo se CA EEM trova una corrispondenza.

Gli amministratori possono contribuire a proteggere il prodotto da un accesso non autorizzato chiedendo agli utenti di modificare periodicamente la password e sospendendo o disattivando gli account predefiniti. Per ulteriori informazioni, consultare:

- Modifica della password in CA EEM (a pagina 46)
- Sospensione o disabilitazione di un account utente (a pagina 40)

**Autorizzazione e protezione basata sui ruoli**

Il prodotto utilizza CA EEM per autorizzare gli utenti che hanno eseguito l'accesso. CA EEM consente agli utenti di eseguire attività solo su quelle parti dell'interfaccia utente per cui sono autorizzati. L'autorizzazione per i gruppi PAMAdmins, Responsabili di progettazione e Utenti dell'ambiente di produzione è presente per impostazione predefinita. Gli utenti aggiunti a questi gruppi ereditano l'autorizzazione.

Gli amministratori possono definire la protezione basata sui ruoli in modo che gli utenti che appartengono a gruppi diversi accedano solo alle parti del prodotto necessarie per il ruolo che eseguono. Gli amministratori possono anche utilizzare le policy di CA EEM per assegnare gli utenti attendibili alle attività che, se utilizzate impropriamente, possono causare ingenti danni. Questo aspetto del controllo di accesso è un fattore separato dal ruolo di gruppo al quale i singoli utenti sono assegnati.

**Ulteriori informazioni:**

Autenticazione e autorizzazione utente in modalità FIPS (a pagina 393)

## Sospensione o disabilitazione di un account utente

È possibile sospendere o disattivare un account utente nei seguenti casi:

- L'accesso dell'utente a CA Process Automation non è più necessario, tuttavia il record deve essere conservato a scopo di audit.
- Sono presenti motivi per cui si desdiera impedire in modo temporaneo o definitivo l'accesso a CA Process Automation per un utente specifico.
- Le credenziali predefinite fornite al momento dell'installazione ora rappresentano una minaccia per la protezione interna. Dal momento che le credenziali per pamadmin e pamuser sono documentate, è consigliabile renderle non disponibili una volta che abbiano esaurito la propria utilità.

**Attenersi alla procedura seguente:**

1. Effettuare l'accesso a CA EEM.
2. Fare clic sull'opzione relativa alla gestione delle identità.
3. Nella funzionalità di ricerca utenti, selezionare Informazioni su utente applicazione e fare clic su Vai.
4. Fare clic sul nome dell'utente di destinazione.
5. Scorrere fino all'area Autenticazione ed effettuare una delle seguenti operazioni:
   - Fare clic su Sospeso.
   - Fare clic sull'opzione della data di disabilitazione, selezionare la data alla quale la disabilitazione diventerà effettiva, quindi fare clic su OK.
6. Fare clic su Salva.

**Nota:** è possibile annullare la sospensione o abilitare un account disabilitato. La funzionalità di disabilitazione/abilitazione permette di rendere disponibile un nuovo account nel momento esatto in cui serve.

## Protezione del trasferimento di dati con crittografie forti

Se i componenti di CA Process Automation vengono installati su macchine virtuali Java, quali ad esempio Java 6, è possibile utilizzare crittografie di livello medio e debole nelle comunicazioni con gli agenti. Per proteggere queste comunicazioni, aggiungere valori di crittografia forte al file di proprietà Oasis.Config nella seguente directory:

`install_dir\server/c2o\config\`

Le proprietà seguenti fanno riferimento alle crittografie utilizzate nelle comunicazioni SSL:

**jboss.ssl.ciphers**

Specifica un elenco di crittografie separato da virgole da utilizzare per la comunicazione SSL tra l'orchestrator di dominio e i client, quali browser e servizi Web. L'elenco di crittografia può variare in base al sistema operativo e al computer virtuale Java presenti sull'host. L'esempio seguente mostra una specificazione tipica di crittografia forte JBoss:

```
jboss.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DS
S_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE
_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA
```

**jetty.ssl.ciphers**

Specifica un elenco di crittografie separato da virgole da utilizzare per le comunicazioni SSL con gli agenti. Il prodotto aggiunge questa proprietà agli agenti durante l'installazione invisibile all'utente. L'esempio seguente mostra una specificazione tipica di crittografia Jetty:

```
jetty.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA
```

## Protezione del trasferimento di dati tra CA Process Automation e CA EEM

CA Process Automation utilizza la crittografia per proteggere i dati archiviati e trasmessi. Se è attiva la modalità FIPS di CA EEM, CA Process Automation protegge i dati archiviati e trasmessi con moduli crittografati conformi a FIPS-140-2.

**Ulteriori informazioni:**

Supporto per FIPS 140-2 (a pagina 391)
Casi di utilizzo della crittografia in CA Process Automation (a pagina 391)

## Tipi di autenticazione

CA EEM esegue l'autenticazione e l'autorizzazione di tutti gli utenti che eseguono l'accesso a CA Process Automation. CA EEM può eseguire l'autenticazione degli utenti nei seguenti modi:

- Mediante le credenziali immesse dagli utenti nel modulo della finestra di dialogo di accesso.
- Mediante il protocollo NTLM, nel caso in cui l'autenticazione pass-through NTLM sia configurata. Questa funzionalità viene spesso selezionata quando CA EEM è configurato per l'utilizzo di Microsoft Active Directory come directory esterna. Le credenziali utente vengono caricate automaticamente in CA EEM per questa configurazione.

Quando un utente accede a CA Process Automation, l'orchestrator determina il tipo di autenticazione da utilizzare:

**Basato sul modulo**

Viene visualizzata la pagina di accesso a CA Process Automation. Dopo aver immesso le credenziali viene avviata l'elaborazione dell'accesso.

**NTLM**

Il protocollo NTLM autentica l'utente sul server CA EEM e viene visualizzata la pagina iniziale.

# Capitolo 3: Amministrazione della protezione di base di CA EEM

Quando si installa CA Process Automation o si esegue l'aggiornamento, CA Process Automation viene registrato con CA EEM. CA EEM offre servizi di gestione delle norme di accesso, autenticazione e autorizzazione per molti prodotti CA Technologies. L'amministrazione della protezione varia a seconda che si tratti della prima configurazione della protezione o dell'esecuzione di un aggiornamento di CA Process Automation. Se si sta eseguendo l'aggiornamento, i requisiti di protezione dipendono dal servizio utilizzato in precedenza per l'autenticazione dell'utente, ovvero CA EEM o LDAP. Se si sta eseguendo una nuova configurazione o un aggiornamento e si desidera caricare gli account utente da un directory server esterno in CA EEM, sarà necessario eseguire un insieme diverso di procedure.

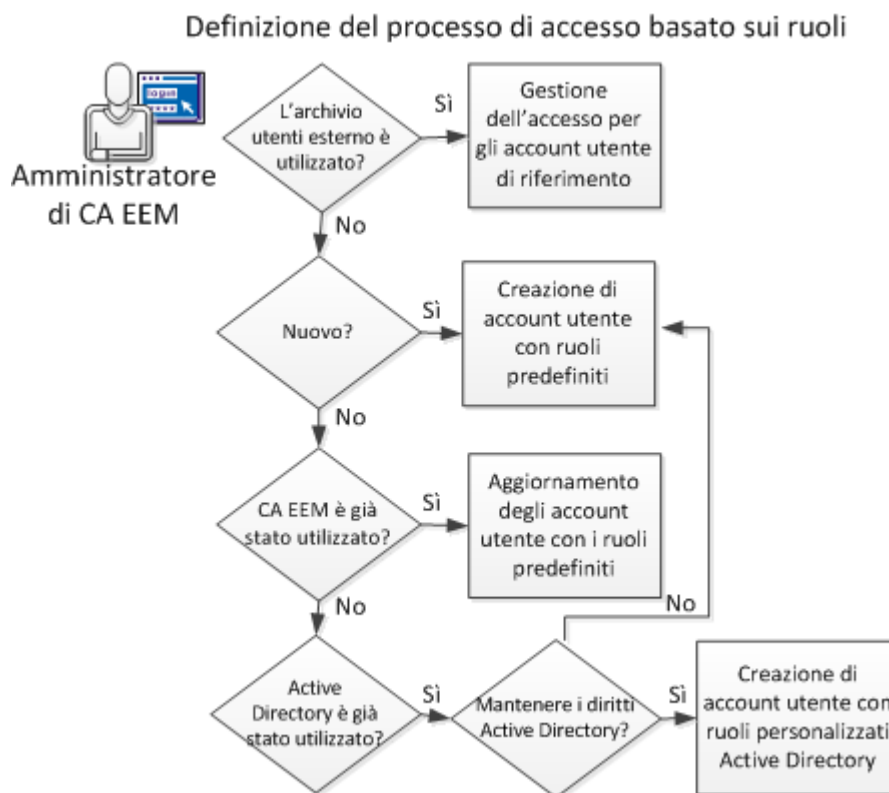
Questo capitolo descrive la procedura utilizzata in CA EEM per assegnare a ciascun utente uno dei quattro ruoli predefiniti in account utenti esistenti, durante la creazione di account utenti o in caso di caricamento degli account utenti da una directory esterna.

In caso di creazione di ruoli e norme personalizzati, consultare la sezione Gestione della protezione avanzata di CA EEM (a pagina 73).

Questa sezione contiene i seguenti argomenti:

# Definizione del processo per l'accesso basato sui ruoli

L'amministrazione della protezione con CA EEM varia in base agli scenari seguenti:

- Nuova installazione o installazione di aggiornamento con un directory server di riferimento: configurazione di CA EEM per l'autenticazione basata sulle credenziali caricate in CA EEM come account utente globale da un archivio utente esterno. È possibile assegnare un gruppo di applicazioni a ciascun utente globale, riflettendo il ruolo eseguito in CA Process Automation.
- Nuova installazione con prodotto CA EEM locale: è possibile definire gli utenti di CA Process Automation in CA EEM.
- Installazione di aggiornamento in caso di utilizzo CA EEM: è possibile aggiornare gli account per gli utenti che progettano i processi o che utilizzano i processi trasferiti nell'ambiente di produzione. Aprire ciascun account e selezionare uno dei nuovi gruppi applicazione: responsabili di progettazione o utenti dell'ambiente di produzione.
- Installazione di aggiornamento in caso di utilizzo di Microsoft Active Directory o un server LDAP simile. È possibile creare gli account per gli utenti esistenti in CA EEM, nonché assegnare agli utenti un gruppo predefinito oppure creare gruppi personalizzati per conservare i ruoli utilizzati con Active Directory.

In base al risultato del diagramma delle decisioni, consultare la sezione appropriata:

- Gestione dell'accesso per account utente di riferimento (a pagina 61).
- Creazione di account utente con ruoli predefiniti (a pagina 54).
- Aggiornamento di account utente con ruoli predefiniti (a pagina 60).
- Creazione di account utente con ruoli Active Directory personalizzati.

  Consultare Transizione dei ruoli utilizzati in Active Directory a CA EEM (a pagina 114).

## Ricerca di CA EEM e accesso

Per gestire gli utenti, i gruppi utenti e i criteri che concedono le autorizzazioni in CA Process Automation, accedere all'applicazione configurata in CA EEM.

**Attenersi alla procedura seguente:**

1. Selezionare CA EEM utilizzato da CA Process Automation. Utilizzare l'URL seguente:

   `https://`*`hostname`*`:5250/spin/eiam`

   Viene visualizzata la finestra di dialogo CA Embedded Entitlements Manager.

2. Dall'elenco a discesa Applicazione, selezionare il nome configurato nel campo Nome applicazione EEM durante l'installazione.

   **Nota:** Il nome predefinito è Process Automation.

3. Immettere uno dei set di credenziali seguenti:

   - Digitare **l'EiamAdmin** e la password dell'amministratore di CA EEM stabilita durante il processo di installazione.
   - Digitare il nome utente e la password se l'amministratore di CA EEM ha concesso l'accesso a CA EEM. L'amministratore di CA EEM può concedere l'accesso a CA EEM ad amministratori selezionati (a pagina 75).

4. Fare clic su Accedi.

# Utilizzo di CA EEM per la modifica della password di CA Process Automation

Generalmente, l'amministratore assegna una password temporanea durante la configurazione degli account per l'archivio utenti interno. Tutti gli utenti di CA Process Automation con account utenti creati in CA EEM possono modificare questa password prima di accedere a CA Process Automation. Quindi, è possibile modificare la password di CA Process Automation nell'intervallo definito dai criteri di password.

**Nota:** Questa capacità non si applica quando CA EEM fa riferimento agli account utenti di un archivio utenti esterno come Microsoft Active Directory. In questo caso, mantenere la password all'interno della directory di riferimento.

Utilizzare CA EEM per modificare la password di CA Process Automation.

**Attenersi alla procedura seguente:**

1. Aprire il browser e immettere l'URL del server di CA EEM utilizzato da CA Process Automation. Ad esempio:
   **https://***hostname_or_IPaddress***:5250/spin/eiam/**

   Per identificare il nome host o l'indirizzo IP di CA EEM utilizzato da CA Process Automation, controllare il campo Server di backend CA EEM nella scheda Configurazione di CA Process Automation, sottoscheda Protezione.

2. Accedere a CA Embedded Entitlements Manager (CA EEM) dalla finestra di dialogo di accesso:

   a. Per Applicazione, selezionare <Global>.

   b. Eliminare EiamAdmin se questo nome predefinito viene visualizzato nel campo Nome utente.

   c. Immettere il nome utente e la password di CA Process Automation.

   d. Fare clic su Accedi.

3. Dalla casella Amministrazione automatica, fare clic su Modifica password.

4. Reimpostare la password:

   a. Immettere il nome utente e la password di CA Process Automation precedente.

   b. Immettere la nuova password in entrambi i campi Nuova password e Conferma password.

   c. Fare clic su OK.

   CA Process Automation accetta le credenziali aggiornate in fase di accesso.

# Accesso basato sui ruoli alla configurazione

L'accesso basato sui ruoli viene implementato in CA EEM, dove PAMAdmins (per amministratori), Responsabili di progettazione e Utenti dell'ambiente di produzione sono tre gruppi specifici dell'applicazione. A ciascun gruppo vengono concesse le autorizzazioni di accesso solo alle funzionalità attinenti al rispettivo ruolo. È possibile utilizzare il quarto gruppo predefinito, PAMUsers, come base per i gruppi personalizzati, se applicabile.

**PAMAdmins (Amministratori)**

Gli amministratori dispongono dell'accesso completo alla scheda Configurazione. Gli amministratori configurano le impostazioni a tutti i livelli della gerarchia di dominio. I riquadri Installazione e Gestisci risorse utente sono presenti solo nella scheda Configurazione degli utenti che sono amministratori.

**Responsabili di progettazione**

CA EEM concede agli utenti nel gruppo dei responsabili di progettazione la possibilità di visualizzare il browser di configurazione e le impostazioni di configurazione nella scheda Configurazione. I responsabili di progettazione dei contenuti di contenuto possono verificare se determinati agenti non sono stati eseguiti correttamente o se una categoria specifica di operatori è disabilitata su un dato touchpoint.

**Utenti dell'ambiente di produzione**

CA EEM concede agli utenti nel gruppo degli utenti dell'ambiente di progettazione la possibilità di visualizzare la scheda Configurazione.

# Gruppi predefiniti e credenziali utente predefinite

CA EEM offre quattro gruppi predefiniti per CA Process Automation. Ciascun gruppo dispone di un utente predefinito. Per verificare la visualizzazione di CA Process Automation per gli utenti di ciascun gruppo, eseguire l'accesso a CA Process Automation come utente predefinito. Di seguito si riporta una descrizione generale e le credenziali degli utenti predefiniti:

**PAMAdmins**

Il gruppo PAMAdmins dispone dei diritti di accesso completi per CA Process Automation. È possibile assegnare a questo gruppo tutti gli amministratori.

**Credenziali utente predefinito**

Nome utente: pamadmin

Password: pamadmin

**Responsabili di progettazione**

Il gruppo Responsabili di progettazione dispone delle autorizzazioni necessarie per gli utenti che progettano i processi automatizzati.

**Credenziali utente predefinito**

Nome utente: pamdesigner

Password: pamdesigner

**Utenti dell'ambiente di produzione**

Il gruppo Utenti ambiente di produzione dispone delle autorizzazioni necessarie per gli utenti che interagiscono con i processi automatizzati nell'ambiente di produzione.

**Credenziali utente predefinito**

Nome utente: pamproduser

Password: pamproduser

**PAMUsers**

Il gruppo PAMUsers predefinito dispone delle autorizzazioni minime. L'amministratore di CA EEM può utilizzare questo gruppo come base per i gruppi personalizzati. Questo gruppo consente di accedere a CA Process Automation, esaminare report e visualizzare lo stato delle operazioni.

**Credenziali utente predefinito**

Nome utente: pamuser

Password: pamuser

Di seguito sono riportate le descrizioni dettagliate relative alle autorizzazioni:

- Autorizzazioni del gruppo PAMAdmins (a pagina 49).
- Autorizzazioni del gruppo Responsabili di progettazione (a pagina 50).
- Autorizzazioni del gruppo Utenti ambiente di produzione (a pagina 52).
- Autorizzazioni del gruppo PAMUsers (a pagina 53).

La modifica dei ruoli predefiniti o la creazione di personalizzati è una funzionalità avanzata.

## Autorizzazioni del gruppo PAMAdmins

I criteri di CA EEM concessi da CA Process Automation forniscono tutte le autorizzazioni al gruppo applicazione PAMAdmins. Assegnare questo gruppo agli amministratori che necessitano dell'accesso completo a CA Process Automation. Il gruppo PAMAdmins concede l'accesso ai seguenti livelli di scheda:

**Pagina iniziale**

Gli amministratori nel gruppo PAMAdmins dispongono dell'accesso completo alla scheda Pagina iniziale. L'accesso completo consente di accedere a CA Process Automation e di utilizzare la scheda Pagina iniziale (policy Accesso utente di PAM40).

**Libreria**

Gli amministratori nel gruppo PAMAdmins dispongono dell'accesso completo alla scheda Pagina iniziale, che include le autorizzazioni seguenti:

- Visualizzazione della scheda Libreria (policy LibraryBrowser di PAM40).
- Controllo delle cartelle di libreria e dei relativi contenuti (diritti Environment_Library_Admin nella policy Ambiente di PAM40).
- Configurazione delle variabili comuni a un gruppo di operatori personalizzati e pubblicazione della configurazione del gruppo nella scheda Moduli del riquadro Browser di configurazione (policy Configurazione del gruppo di PAM40).

**Progettazione**

Gli amministratori nel gruppo PAMAdmins dispongono dell'accesso completo alla scheda Progettazione, che include le autorizzazioni seguenti:

- Visualizzazione della scheda Progettazione (policy Progettazione).
- Diritti completi nella scheda Progettazione (diritti Environment_Library_Admin nella policy Ambiente di PAM40).

**Operazioni**

Gli amministratori nel gruppo PAMAdmins dispongono dell'accesso completo alla scheda Operazioni, che include le autorizzazioni seguenti:

- Visualizzazione di tutti i riquadri nella scheda Operazioni (policy Operazioni di PAM40).
- Autorizzazioni complete (diritti Environment_Library_Admin nella policy Ambiente di PAM40).

**Configurazione**

Gli amministratori nel gruppo PAMAdmins dispongono dell'accesso completo alla scheda Configurazione, che include le autorizzazioni seguenti:

- Visualizzazione di tutti i riquadri nel riquadro Browser di configurazione (policy Configurazione di PAM40).
- Configurazione a livello di dominio o esecuzione di un'attività che richiede il blocco del dominio (policy Dominio di PAM40).
- Configurazione a livello di ambiente o esecuzione di un'attività che richiede il blocco di un ambiente (diritti Environment_Config_Admin della policy Ambiente di PAM40).
- Installazione di agenti o orchestrator (policy Configurazione di PAM40).
- Gestione delle risorse utente (policy Configurazione di PAM40).

**Report**

Gli amministratori nel gruppo PAMAdmins dispongono dell'accesso completo alla scheda Report. L'accesso completo include le autorizzazioni di visualizzazione della scheda Report, di generazione dei report e di aggiunta di nuovi report (policy Report di PAM40).

## Autorizzazioni del gruppo dei responsabili di progettazione

Per impostazione predefinita, il gruppo applicazione dei responsabili di progettazione contiene le autorizzazioni di cui necessitano gli utenti nell'ambiente di progettazione. Il gruppo dei responsabili di progettazione concede l'accesso ai seguenti livelli di scheda:

**Pagina iniziale**

Gli utenti nel gruppo dei responsabili di progettazione possono eseguire l'accesso a CA Process Automation e utilizzare la scheda Pagina iniziale (policy Accesso utente di PAM40).

**Libreria**

Gli utenti nel gruppo dei responsabili di progettazione dispongono del seguente tipo di accesso alla scheda Libreria:

- Visualizzazione della scheda Libreria (policy LibraryBrowser di PAM40).
- Lettura della scheda Libreria, comprese le autorizzazioni di visualizzazione, esportazione e ricerca degli oggetti di automazione (policy Ambiente di PAM40).
- Controllo (visualizzazione, esplorazione, modifica, eliminazione, creazione) delle cartelle nella scheda Libreria e controllo degli oggetti di automazione nei rispettivi editor (policy Oggetto di PAM40).

**Progettazione**

Gli utenti nel gruppo dei responsabili di progettazione dispongono del seguente tipo di accesso alla scheda Progettazione:

- Visualizzazione della scheda Progettazione (policy Progettazione di PAM40).
- Progettazione di processi automatizzati e controllo (visualizzazione, esplorazione, modifica, eliminazione e creazione) di tutti gli oggetti di automazione nei rispettivi editor. La scheda Progettazione costituisce l'editor dell'oggetto di Process Automation (policy Oggetto di PAM40).

**Operazioni**

Gli utenti nel gruppo dei responsabili di progettazione dispongono del seguente tipo di accesso alla scheda Operazioni:

- Visualizzazione di tutti i riquadri nella scheda Operazioni (policy Operazioni di PAM40).
- Controllo delle pianificazioni visualizzate nella scheda Operazioni (policy Pianificazione di PAM40).
- Verifica e modifica dell'oggetto di automazione set di dati (policy Set di dati di PAM40).
- Controllo, avvio e monitoraggio dell'oggetto di automazione del processo (policy Processo di PAM40).
- Controllo dell'oggetto di automazione risorse (policy Risorse di PAM40).
- Avvio e rimozione dalla coda della policy del modulo di richiesta di avvio (policy Modulo di richiesta di avvio di PAM40).
- Visualizzazione della versione di rilascio di un pacchetto di contenuto importato e degli oggetti al suo interno.

**Configurazione**

Gli utenti nel gruppo dei responsabili di progettazione possono visualizzare le schede di qualsiasi nodo selezionato nel riquadro Browser di configurazione (policy Configurazione di PAM40).

**Report**

Gli utenti nel gruppo dei responsabili di progettazione possono visualizzare la scheda Report, generare e aggiungere report. Il gruppo dei responsabili di progettazione si basa sul gruppo PAMUsers, che dispone anch'esso di tali autorizzazioni.

## Autorizzazioni del gruppo degli utenti dell'ambiente di produzione

Per impostazione predefinita, il gruppo applicazione degli utenti dell'ambiente di produzione contiene le autorizzazioni di cui necessitano gli utenti nell'ambiente di produzione. Il gruppo degli utenti dell'ambiente di produzione concede l'accesso ai seguenti livelli di scheda:

**Pagina iniziale**

Gli utenti assegnati al gruppo degli utenti dell'ambiente di produzione possono accedere a CA Process Automation e utilizzare la scheda Pagina iniziale (policy Accesso utente di PAM40).

**Libreria**

Gli utenti nel gruppo degli utenti dell'ambiente di produzione dispongono del seguente tipo di accesso alla scheda Libreria:

- Visualizzazione della scheda Libreria (policy LibraryBrowser di PAM40).
- Lettura dalla scheda Libreria (policy Ambiente di PAM40, prerequisito per la policy Oggetto di PAM40).
- Esplorazione della struttura di cartella nella scheda Libreria e visualizzazione degli oggetti di automazione elencati in ciascuna cartella (policy Oggetto di PAM40).

**Operazioni**

Gli utenti nel gruppo degli utenti dell'ambiente di produzione dispongono del seguente tipo di accesso alla scheda Operazioni:

- Visualizzazione di tutti i riquadri nella scheda Operazioni (policy Operazioni di PAM40).
- Controllo delle pianificazioni visualizzate nella scheda Operazioni (policy Pianificazione di PAM40).
- Analisi dei set di dati visualizzati nel riquadro Set di dati della scheda Operazioni (policy Set di dati di PAM40).
- Monitoraggio o avvio dei processi visualizzati nella scheda Operazioni (policy Processo di PAM40).
- Avvio e rimozione dalla coda del modulo di richiesta di avvio visualizzato nella scheda Operazioni (policy Modulo di richiesta di avvio di PAM40).
- Visualizzazione della versione di rilascio di un pacchetto di contenuto importato e degli oggetti al suo interno.

**Configurazione**

Gli utenti nel gruppo degli utenti dell'ambiente di produzione possono visualizzare le schede di qualsiasi nodo selezionato nel riquadro Browser di configurazione (policy Configurazione di PAM40).

**Report**

Gli utenti nel gruppo degli utenti dell'ambiente di produzione possono visualizzare la scheda Report, generare e aggiungere report (policy Report di PAM40).

## Autorizzazioni del gruppo PAMUsers

Per impostazione predefinita, il gruppo applicazione PAMUsers contiene autorizzazioni di base. È possibile utilizzare questo gruppo in aggiunta ai gruppi personalizzati creati per l'accesso specifico basato sui ruoli. Il gruppo PAMUsers concede l'accesso ai seguenti livelli di scheda:

**Pagina iniziale**

Gli utenti nel gruppo PAMUsers possono eseguire l'accesso a CA Process Automation e utilizzare la scheda Pagina iniziale (policy Accesso utente di PAM40).

**Libreria**

Gli utenti nel gruppo PAMUsers dispongono del seguente tipo di accesso alla scheda Libreria:

- Visualizzazione della scheda Libreria (policy LibraryBrowser di PAM40).
- Lettura della scheda Libreria (policy Ambiente di PAM40).

**Operazioni**

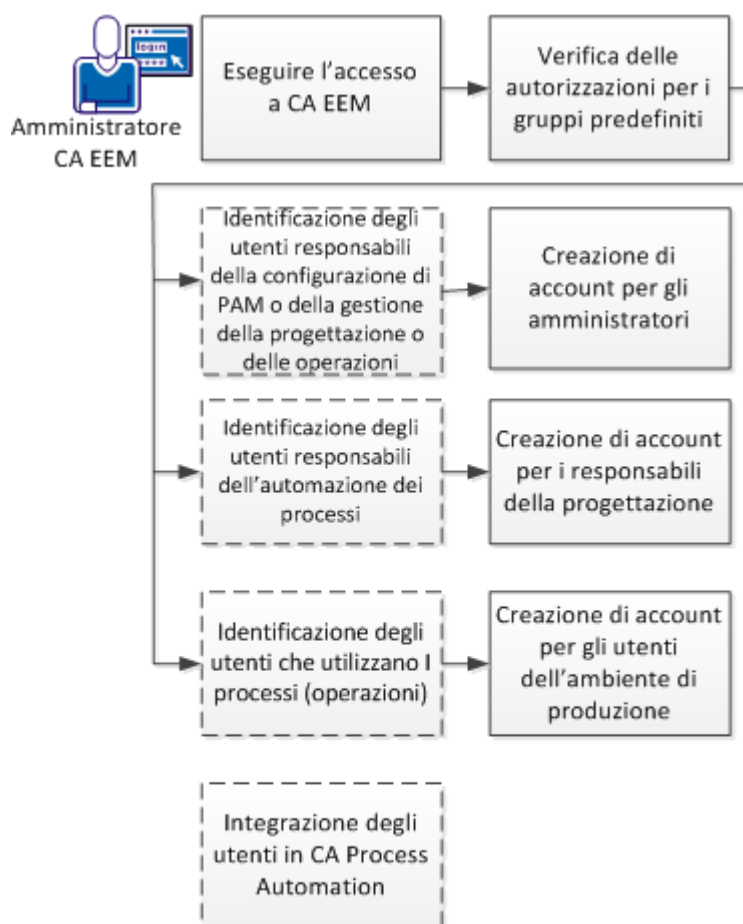
Gli utenti nel gruppo PAMUsers possono visualizzare la scheda Operazioni (policy Operazioni di PAM40).

**Report**

Gli utenti nel gruppo PAMUsers possono visualizzare la scheda Report, generare e aggiungere report (policy Report di PAM40).

# Creazione di account utente con ruoli predefiniti

Quando il programma di installazione configura CA EEM per l'utilizzo dell'archivio utenti interno, l'amministratore di CA EEM crea un account utente per ciascun utente di CA Process Automation. Questi account utenti vengono utilizzati per l'autenticazione degli utenti al momento dell'accesso a CA Process Automation. Per autorizzare questi utenti ad accedere alle funzionalità necessarie per i relativi ruoli, l'amministratore di CA EEM assegna il gruppo predefinito appropriato a ciascun account utente.

La figura seguente mostra la procedura per creare account utente con ruoli predefiniti. Le linee tratteggiate indicano le attività eseguite all'esterno di CA Process Automation.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Verifica delle autorizzazioni per i gruppi predefiniti.
   - Autorizzazioni del gruppo PAMAdmins (a pagina 49)
   - Autorizzazioni del gruppo dei responsabili di progettazione (a pagina 50)
   - Autorizzazioni del gruppo degli utenti dell'ambiente di produzione (a pagina 52)
   - Autorizzazioni del gruppo PAMUsers (a pagina 53)
3. Creazione di un account utente per amministratori (a pagina 55).
4. Creazione di account utente per responsabili di progettazione (a pagina 56).
5. Creazione di account utente per utenti dell'ambiente di produzione. (a pagina 57)
6. Introduzione di CA Process Automation a nuovi utenti (a pagina 59).

## Creazione di account utente per amministratori

Gli amministratori richiedono l'accesso completo a tutte le funzionalità di CA Process Automation. Per concedere questo accesso, associare gli account utente per amministratori al gruppo PAMAdmins.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestione identità.
3. Nel riquadro Utenti, fare clic sull'icona accanto a Utenti.

   Viene visualizzata la pagina Nuovo utente.
4. Nel campo Nome utente, digitare l'ID utente da assegnare all'account utente.

   L'utente digita questo valore nel campo Nome utente quando effettua l'accesso.
5. Fare clic su Aggiungi informazioni sull'utente dell'applicazione.

   Il riquadro viene aggiornato per mostrare la sezione Appartenenza gruppo applicazione.
6. Selezionare PAMAdmins da Gruppi utenti disponibili e fare clic su > per spostarlo in Gruppo utenti selezionato.
7. Immettere i dettagli dell'utente globale.
   a. Immettere il nome nei campi Nome e Cognome.

      La barra del titolo visualizza questi valori quando l'utente accede a CA Process Automation.

   b. Compilare gli altri campi necessari nell'area Generale.

8. (Facoltativo) Se si utilizza CA Process Automation con un altro prodotto di CA Technologies che utilizza CA EEM, completare la sezione Appartenenza gruppo globale.

9. Fornire le informazioni di autenticazione temporanea per questo account utente:

   a. Selezionare Modifica password all'accesso successivo.

   b. Immettere una password temporanea nel campo Nuova password.

   c. Inserire la stessa password temporanea nel campo Conferma password.

10. (Facoltativo) Compilare i campi restanti nella pagina Nuovo utente.

11. Fare clic su Salva, quindi su Chiudi.

12. (Facoltativo) Fare clic su Disconnetti.

**Ulteriori informazioni:**

Utilizzo di CA EEM per la modifica della password di CA Process Automation (a pagina 46)
Concessione dell'accesso a CA EEM ad amministratori specifici (a pagina 75)

## Creazione di account utente per i responsabili di progettazione

Creare un account utente per ciascun responsabile di progettazione che richiede l'accesso agli oggetti di automazione in CA Process Automation. Gli oggetti di automazione vengono utilizzati per automatizzare i processi.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).

2. Fare clic sulla scheda Gestisci identità.

3. Fare clic su Nuovo utente.

   Viene visualizzata la pagina Nuovo utente.

4. Immettere l'ID utente da assegnare all'account utente nel campo Nome.

5. Fare clic su Aggiungi informazioni su utente applicazione.

6. Selezionare il gruppo Responsabili di progettazione dai gruppi di utenti disponibili e fare clic su > per spostarlo nei gruppi di utenti selezionati.
7. Immettere i dettagli dell'utente globale.
8. Immettere e verificare una password.

   Gli utenti possono modificare le rispettive password in CA EEM.
9. (Facoltativo) Completare i campi restanti nella pagina Nuovo utente.
10. Fare clic su Salva, quindi su Chiudi.
11. Fare clic su Disconnetti.

## Creazione di account utente per utenti dell'ambiente di produzione

Creare un account utente per ciascun utente dell'ambiente di produzione che richiede l'accesso a CA Process Automation per monitorare e interagire con i processi automatizzati.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestisci identità.
3. Fare clic su Nuovo utente.

   Viene visualizzata la pagina Nuovo utente.
4. Immettere l'ID utente da assegnare all'account utente nel campo Nome.
5. Fare clic su Aggiungi informazioni su utente applicazione.
6. Selezionare il gruppo Utenti ambiente di produzione dai gruppi di utenti disponibili e fare clic su > per spostarlo nei gruppi di utenti selezionati.
7. Immettere i dettagli dell'utente globale.
8. Immettere e verificare una password.

   Gli utenti possono modificare le rispettive password in CA EEM.
9. (Facoltativo) Completare i campi restanti nella pagina Nuovo utente.
10. Fare clic su Salva, quindi su Chiudi.
11. Fare clic su Disconnetti.

## Creazione di account utente con accesso di base

*PAMUsers* è un gruppo predefinito che consente l'utilizzo delle schede Pagina iniziale e Report e garantisce l'accesso in sola lettura alle schede Libreria e Operazioni. Un utente che dispone solo dell'accesso PAMUsers può acquisire dimestichezza con il prodotto, ma non può creare o configurare gli oggetti.

Utilizzare questo gruppo come base per i gruppi personalizzati.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestione identità.
3. Fare clic su Nuovo utente.
4. Immettere l'ID utente da assegnare all'account utente nel campo Nome.
5. Fare clic su Aggiungi informazioni sull'utente dell'applicazione, quindi fare clic su > per spostare PAMUsers in Gruppi utenti selezionato.
6. Immettere i dettagli dell'utente globale.
7. Immettere e verificare una password.

   Gli utenti possono accedere a CA EEM con le credenziali di CA Process Automation e modificare la propria password.
8. (Facoltativo) Compilare i campi restanti nella pagina Nuovo utente.
9. Fare clic su Salva, quindi su Chiudi.
10. Fare clic su Disconnetti.

# Introduzione di CA Process Automation a nuovi utenti

Per aiutare i nuovi utenti a diventare produttivi, fornire loro le informazioni seguenti:

**Informazioni di accesso**

- L'URL di CA Process Automation. Potrebbe essere l'URL dell'orchestrator di dominio o l'URL dell'utilità di bilanciamento del carico per l'orchestrator di dominio. Eventualmente è possibile accedere all'URL di qualsiasi orchestrator specificato.
- Informazioni di accesso. Gli utenti accedono utilizzando il nome utente e la password configurati nel proprio account utente di CA EEM.
- L'URL di CA EEM. Gli utenti accedono utilizzando il nome utente e la password assegnati, quindi si auto-assegnano una nuova password.

  **Nota:** Se CA EEM fa riferimento a uno o più Microsoft Active Directory esterni, non è necessario eseguire l'accesso a CA EEM. Le password vengono gestite con Active Directory.

**Accesso alle risorse per velocizzare la fase introduttiva**

- Consigliare agli utenti di completare i tutorial di CA Process Automation accessibili dalla scheda Pagina iniziale.
- Mostrare agli utenti come è possibile accedere al bookshelf selezionando l'opzione Bookshelf dal collegamento Guida in linea nella barra degli strumenti. Dal bookshelf, gli utenti possono accedere alle guide per il loro ruolo.

  Le guide per ciascun gruppo applicazione (ruolo) sono:

  PAMAdmins

  *Note di rilascio*

  *Guida all'installazione*

  *Guida per l'amministratore del contenuto*

  *Guida di riferimento all'interfaccia utente*

  Responsabili di progettazione

  *Guida alla progettazione dei contenuti*

  *Guida di riferimento per la progettazione dei contenuti*

  *Guida di riferimento per le API dei servizi Web*

  *Guida per l'utente dell'ambiente di produzione*

  *Guida di riferimento all'interfaccia utente*

  Utenti dell'ambiente di produzione

  *Guida per l'utente dell'ambiente di produzione*

  *Guida di riferimento all'interfaccia utente*

# Aggiornamento degli account utente con ruoli predefiniti

L'aggiornamento degli utenti precedentemente assegnati a PAMAdmins (o ITPAMAdmins) come gruppo dei responsabili di progettazione o degli utenti dell'ambiente di produzione può contribuire al miglioramento della protezione. Si consiglia agli utenti aggiornati di considerare l'assegnazione dei seguenti gruppi predefiniti agli utenti che eseguono i ruoli seguenti:

- Responsabili di progettazione
- Utenti dell'ambiente di produzione

**Nota:** se in precedenza PAMUsers (o ITPAMUsers) sono stati assegnati agli account utente di persone che hanno lavorato con Elenchi attività, Visualizzazione predefinita processo o Richieste utente, riassegnare il gruppo degli utenti dell'ambiente di produzione a questi account.

**Attenersi alla procedura seguente:**

1. Cercare CA EEM ed eseguire l'accesso (a pagina 45).
2. Fare clic sulla scheda Gestisci identità.
3. Espandere il riquadro Cerca utenti, selezionare Application Users (Utenti applicazione), inserire i criteri seguenti, quindi fare clic su Vai.
   - Attributo: appartenenza gruppo
   - Operatore: UGUALE A
   - Valore: PAMAdmins

   Viene visualizzato l'elenco degli account utente attualmente assegnati al gruppo PAMAdmins.
4. Fare clic sul nome di un utente che ricopre il ruolo di responsabile di progettazione o utente dell'ambiente di produzione.

   Viene visualizzato l'account utente selezionato.
5. Selezionare PAMAdmins da Gruppo utenti selezionati e fare clic sulla freccia sinistra

   Il gruppo selezionato viene rimosso da Gruppo utenti selezionati.
6. Selezionare il gruppo applicabile dai gruppi di utenti disponibili e fare clic su > per spostarlo nei gruppi di utenti selezionati.
   - Per i responsabili di progettazione dei contenuti, selezionare Responsabili di progettazione.
   - Per gli utenti dell'ambiente di produzione, selezionare Production Users (Utenti dell'ambiente di produzione).
7. Fare clic su Salva, quindi su Chiudi.
8. Fare clic su Disconnetti.

# Gestione dell'accesso per gli account utente di riferimento

Se si fa riferimento a un archivio utente esterno durante l'installazione di CA EEM, i gruppi globali e gli account utente vengono caricati automaticamente in CA EEM. CA Process Automation consente il caricamento di un numero massimo di 10.000 account con un parametro configurabile che estende l'impostazione di 2000 di CA EEM. Per informazioni sulla personalizzazione di questa impostazione, consultare Impostazione del numero massimo di utenti e gruppi di CA EEM (a pagina 62).

Gli account utente di un archivio utenti di riferimento esterno vengono caricati come record di sola lettura. Se un nuovo utente richiede un account, crearlo nell'archivio utente esterno. Il nuovo record viene caricato automaticamente. È possibile consentire l'accesso a CA Process Automation a livello di gruppo globale o di utente globale.

CA EEM viene configurato per concedere l'accesso a CA Process Automation e ai relativi componenti, tuttavia l'autenticazione viene gestita dall'archivio utente di riferimento. Per accedere a CA Process Automation, gli utenti globali con diritti di accesso utilizzano il nome utente e la password (o il nome principale e la password) nell'archivio utenti di riferimento.

**Nota:** non è possibile utilizzare CA EEM per aggiornare i record utente memorizzati in un archivio utente esterno.

Per gestire l'accesso di utenti con account archiviati in un archivio utente esterno, valutare le procedure seguenti.

- Aggiungere un gruppo di applicazioni per ogni account utente globale.

  Cercare ciascun utente globale per nome. Assegnare all'account utente globale uno dei gruppi applicazione predefiniti (PAMAdmins, Progettazione, Utenti dell'ambiente di produzione o PAMUsers) o un gruppo personalizzato. È inoltre possibile creare gruppi globali e aggiungervi utenti globali selezionati.

  **Importante.** Immettere sempre i criteri di ricerca per evitare la visualizzazione di tutte le voci presenti in un archivio utente esterno.

- Aggiungere un gruppo globale alle policy di accesso di CA Process Automation e selezionare le azioni da consentire.

  In particolare, aggiungere il gruppo globale alle policy predefinite che forniscono i diritti di accesso desiderati a tutti gli utenti del gruppo. Ad esempio, aggiungere il gruppo globale alla policy Accesso utente di PAM40 per consentire l'accesso a CA Process Automation a tutti gli utenti globali appartenenti a tale gruppo. Per concedere l'accesso alla scheda Progettazione, aggiungere il gruppo alla policy Progettazione di PAM40.

- Creare un gruppo dinamico composto da utenti globali o da gruppi globali selezionati. I gruppi di applicazioni personalizzati possono essere aggiunti a un gruppo dinamico.
- Attenersi alla procedura documentata, Integrazione di Active Directory con CA EEM.

  che concede a tutti gli utenti di Active Directory l'accesso completo a CA Process Automation senza alcuna configurazione in CA EEM. Nonostante sia facile da applicare, questa procedura non offre la protezione dell'accesso basato su ruoli.

**Importante.** Per i server LDAP di terze parti, configurare il parametro seguente nel livello di contesto ou=system:

```
ou=Global Groups
```

**Ulteriori informazioni:**

Assegnare un gruppo di applicazioni a un utente globale (a pagina 69)
Creazione di una policy di gruppo di utenti dinamici (a pagina 70)

## Impostare il numero massimo di utenti e gruppi di CA EEM.

Prima di integrare un ampio archivio utenti di riferimento, determinare se contiene più di 10.000 utenti e gruppi. Il valore predefinito eem.max.search.size (10000) è la soglia per il numero di utenti e gruppi che CA Embedded Entitlements Manager può accettare durante il trasferimento. Il valore predefinito di CA Process Automation (10.000) estende il valore predefinito di CA EEM (2.000).

Aumentare il valore eem.max.search.size se viene visualizzato il messaggio seguente durante la ricerca di utenti disponibili senza definire i criteri di ricerca:

```
Superato il limite massimo di ricerca.
```

Per sostituire la soglia predefinita nel file OasisConfig.properties, impostare il parametro seguente su un valore nuovo:

```
eem.max.search.size = 10000
```

Se si integra una directory di riferimento di grandi dimensioni, impostare un valore superiore a 20000.

**Attenersi alla procedura seguente:**

1. Accedere come amministratore al server in cui l'orchestrator di domino è installato.
2. Accedere alla seguente cartella:

   *install_dir*/server/c2o/.config

   ***install_dir***

   Fa riferimento al percorso in cui è installato l'orchestrator di dominio.
3. Aprire il file OasisConfig.properties con un editor di testo.
4. Utilizzare Trova per individuare il parametro eem.max.search.size.
5. Cambiare il valore da 10000 a un valore appropriato.
6. Salvare il file e chiudere l'editor di testo.
7. Riavviare l'orchestrator:
   a. Interrompere l'orchestrator (a pagina 196).
   b. Avviare l'orchestrator (a pagina 197).

## Ricerca di identità corrispondenti ai criteri specificati

Quando si fa riferimento a un archivio utenti esterno di grandi dimensioni, specificare i criteri di ricerca. I criteri di ricerca limitano i record di account utente globale restituiti al sottoinsieme richiesto o attinente. Ad esempio, specificare **Nome UGUALE A John** per recuperare i nomi di tutti gli utenti con il nome John.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic su Gestione identità.
3. Selezionare Utenti globali nel riquadro Cerca utenti.
4. Rivedere l'elenco a discesa Attributo e determinare se agli attributi elencati sia assegnato un valore per l'utente o per gli utenti che si desiderano cercare.
   - Se sì, selezionare uno o più attributi applicabili. Ad esempio, selezionare Nome e Cognome.
   - In caso contrario, selezionare i puntini di sospensione (...) e immettere il nome dell'attributo in cui eseguire la ricerca.

5. Selezionare l'operatore per l'espressione e immettere un valore per l'attributo che viene applicato agli account utente di destinazione. Il valore può essere un valore parziale. Ad esempio, immettere s* per cercare tutti i record in cui il valore dell'attributo selezionato inizia con la lettera "s".

   **Importante.** Immettere sempre i criteri per la ricerca per ridurre al minimo il tempo impiegato per recuperare le voci da un archivio utente esterno.

6. Fare clic su Vai.

   I nomi degli utenti globali che corrispondono ai criteri di selezione vengono visualizzati nel riquadro Utenti. I nomi vengono visualizzati nel formato Cognome, Nome.

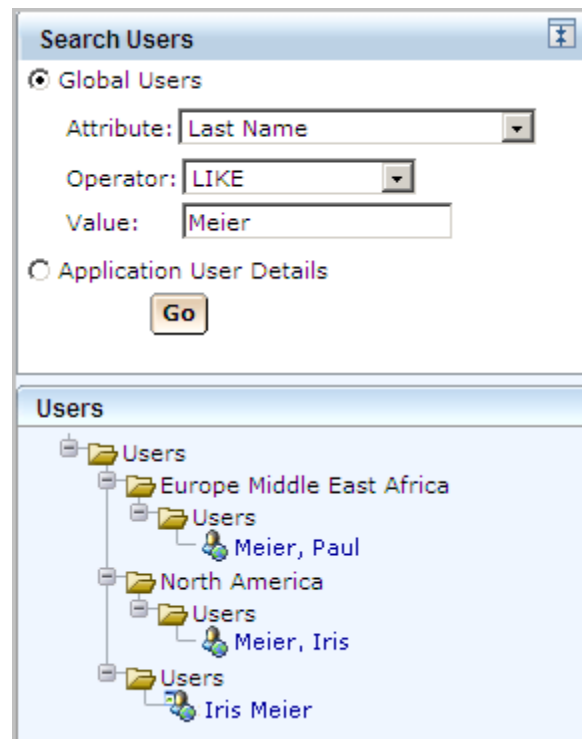
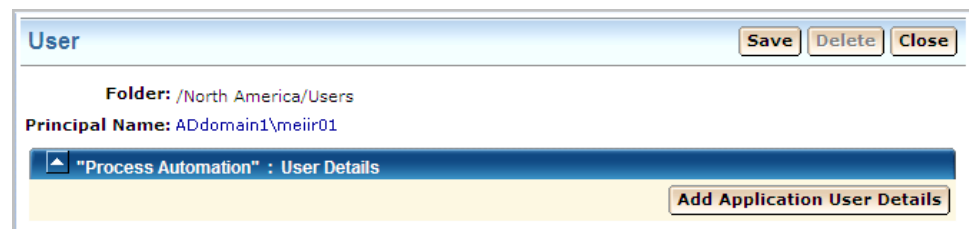
## Esempio: Una singola Active Directory in due Active Directory di riferimento

Presupposti:

- Prima di eseguire l'aggiornamento di CA Process Automation, CA EEM ha fatto riferimento a una directory esterna, una Microsoft Active Directory. Il rilascio di CA EEM era r8.4
- In un secondo momento, ma prima di eseguire l'aggiornamento di CA Process Automation, CA EEM è stato aggiornato dalla versione r8.4 alla versione r12.51. Ovvero, gli utenti di CA Process Automation hanno fatto riferimento agli utenti di Active Directory che erano assegnati a un gruppo applicazione, mantenendo l'assegnazione del gruppo dopo l'aggiornamento di CA EEM. Gli utenti globali assegnati al gruppo dei responsabili di progettazione che era titolare degli oggetti di automazione mantenevano la titolarità dell'oggetto.
- Durante l'aggiornamento di CA Process Automation alla versione r4.2, il programma di installazione ha selezionato di fare riferimento a più Active Directory, una funzionalità supportata a partire da CA EEM r12.5.
- Ora l'amministratore di CA EEM deve assegnare un gruppo utenti applicazione a utenti globali selezionati dalle Active Directory aggiuntive. L'amministratore riassegna anche i gruppi applicazione agli utenti di CA Process Automation dall'Active Directory originale.
- L'amministratore di CA EEM immette i criteri di ricerca per un utente in uno dei domini Active Directory a cui si è fatto riferimento di recente. Risulta che questo utente si trova in due domini, nel dominio esistente e in un nuovo dominio. Benché in genere ciascun utente si trovi in un dominio, è possibile che gli utenti si trovino in più di un dominio Active Directory. In questo caso i due account utente vengono trattati come utenti diversi, anche se potrebbero fare riferimento allo stesso individuo.

La procedura seguente mostra come questo esempio verrebbe visualizzato nei risultati della ricerca di CA EEM e nei record utente corrispondenti.

**Attenersi alla procedura seguente:**

1. Accedere a CA EEM come amministratore di CA EEM.
2. Fare clic su Gestione identità. Immettere i criteri di ricerca per Utenti globali. La ricerca di esempio è per tutti gli utenti di Active Directory con il cognome Meier.

2. Selezionare uno degli utenti globali visualizzati, ad esempio Meier, Iris. Viene visualizzato il riquadro Account utente. Esso rappresenta il record del dominio Active Directory a cui si è fatto riferimento di recente. Fare clic su Aggiungi informazioni sull'utente dell'applicazione.

3. Selezionare il gruppo utenti PAMAdmins per creare le autorizzazioni di amministratore a CA Process Automation per l'utente.

4. Selezionare l'altra voce Utente globale dai risultati della ricerca. Si noti che esso visualizza ADdomain2, non ADdomain1, e che dispone delle autorizzazioni dell'utente dell'ambiente di produzione. Questo rappresenta il record utente esistente.

5. L'utente nel dominio Active Directory a cui si faceva riferimento in origine può accedere a CA Process Automation con il nome utente non completo, se tale dominio è impostato come dominio predefinito. (Tutti gli utenti dei domini aggiuntivi devono immettere il proprio nome principale per Nome utente al momento dell'accesso. Pertanto, nel caso di questo esempio, l'immissione del nome utente non completo comporta l'accesso dell'utente con le autorizzazioni dell'utente dell'ambiente di produzione. Per ottenere l'autorizzazione PAMAdmins, l'utente deve immettere ADdomain1\meiir01 nel campo Nome utente.

## Informazioni sugli utenti globali

Tutti gli utenti definiti in CA EEM sono utenti globali. Gli utenti globali possono corrispondere a uno dei tipi seguenti:

- Utenti per i quali si creano account utente globali, in cui è possibile specificare tutti i dettagli, inclusa l'assegnazione di un gruppo di applicazioni e la scelta di una password.
- Utenti definiti in CA EEM per l'uso con un altro prodotto di CA. Eseguire la ricerca per tali utenti globali e fornire l'accesso a CA Process Automation assegnando un gruppo applicazione di CA Process Automation a ciascun utente. Tali utenti accedono a CA Process Automation con le credenziali precedentemente definite in CA EEM.
- Utenti definiti in un archivio utenti esterno che vengono identificati durante l'installazione di CA EEM. Eseguire la ricerca per tali utenti globali e fornire l'accesso a CA Process Automation assegnando un gruppo applicazione di CA Process Automation a ciascun utente. Tali utenti accedono a CA Process Automation con le credenziali definite nell'archivio utenti esterno.

  **Nota:** Gli utenti immettono le credenziali come il nome principale (*nome di dominio**nome utente*) e la password oppure il nome utente e la password. Il nome principale viene *accettato* quando CA EEM utilizza Microsoft Active Directory come archivio utenti esterno e viene fatto riferimento a più domini durante l'installazione. Il nome principale è *obbligatorio* quando il dominio Active Directory di origine per l'utente non è il dominio predefinito.

Se si utilizza l'archivio utenti interno di CA EEM, si creano utenti globali e si assegnano gruppi applicazione. Se fa riferimento a un archivio utenti esterno, si recuperano utenti globali e si assegnano gruppi applicazione.

## Assegnare un gruppo di applicazioni a un utente globale

Per concedere l'accesso basato sui ruoli a un utente, assegnare un gruppo applicazione al rispettivo account utente globale.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Cercare le identità corrispondenti ai criteri specificati (a pagina 63).
3. In Utenti, selezionare il nome utente di destinazione.

   Viene visualizzato l'account utente selezionato.
4. Fare clic su Aggiungi informazioni sull'utente dell'applicazione.

   Viene visualizzata la finestra di dialogo Appartenenza gruppo applicazione.

5. Selezionare il gruppo appropriato da Gruppi utenti disponibili, quindi fare clic sulla freccia destra (>) per spostarlo in Gruppo utenti selezionato.
6. Fare clic su Salva.

   L'utente globale di destinazione è ora in grado di accedere a CA Process Automation. Dopo il processo di autenticazione, l'utente può accedere alla funzionalità concessa dal prodotto a tutti i membri del gruppo applicazione assegnato.

## Informazioni sui gruppi utenti dinamici

Un *gruppo utenti dinamico* è composto da utenti globali che condividono uno o più attributi. Viene creato attraverso un criterio specifico per il gruppo utenti dinamico. Il nome di risorsa è il nome del gruppo utenti dinamico e l'appartenenza si basa su filtri configurati per attributi di utente e gruppo.

È possibile creare un gruppo utenti dinamico composto da Utenti, Gruppi applicazione, Gruppi globali o Gruppi dinamici. Ad esempio, è possibile creare un gruppo utenti dinamico di gruppi globali o gruppi applicazione basati su nome, descrizione o appartenenza al gruppo. In maniera analoga, è possibile creare un gruppo utenti dinamico di utenti con ruoli diversi basati su un attributo comune nel relativo profilo di utente globale. Ad esempio:

- Qualifica professionale
- Reparto o ufficio
- Città, provincia o paese

L'utente EiamAdmin può creare policy di gruppo di utenti dinamici.

## Creazione di una policy di gruppo di utenti dinamici

È possibile creare una policy per un gruppo utenti dinamico.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic su Gestione criteri di accesso, quindi su Nuovo criterio gruppo dinamico a sinistra di Criteri gruppo utenti dinamico.
3. Per Nome, immettere un nome di gruppo che identifica una proprietà comune del gruppo di utenti. Immettere una descrizione (facoltativo).
4. Selezionare un tipo di policy. Il valore predefinito è Criterio di accesso.

5. Selezionare le identità come segue:

   a. Per Tipo, selezionare uno dei valori seguenti, quindi fare clic su Cerca identità.

      - Utente
      - Gruppo applicazione
      - Gruppo globale
      - Gruppo dinamico

   b. In Attributo, Operatore e Valore, inserire l'espressione che imposta le policy di appartenenza al gruppo e fare clic su Cerca.

      **Esempio:**

      Selezionare Utente, immettere **Professione uguale a Manager** e fare clic su Cerca. Il processo restituisce tutti gli utenti con la professione Manager.

   c. Nei risultati della ricerca, selezionare gli utenti da aggiungere come membri al gruppo dinamico. Per spostare quanto selezionato nell'elenco Identità selezionate, fare clic sulla freccia destra (>).

6. In Azioni, selezionare appartenenza.

7. Nel campo Aggiungi risorsa, immettere il valore immesso nel campo Nome, quindi fare clic su Aggiungi.

   Il processo aggiunge le identità selezionate al gruppo utenti dinamico creato.

8. (Facoltativo) Aggiungere altri filtri.

9. Fare clic su Salva.

   La policy creata viene visualizzata quando si fa clic sul collegamento Criteri gruppo utenti dinamico.

# Capitolo 4: Gestione della protezione avanzata di CA EEM

È possibile utilizzare CA EEM per creare policy di accesso dettagliate e soddisfare requisiti di protezione specifici. È possibile creare policy personalizzate, i gruppi che utilizzano tali policy personalizzate e assegnare i propri gruppi personalizzati ad account utenti. In alternativa, è possibile assegnare gli utenti direttamente alle policy personalizzate. È possibile definire policy personalizzate per limitare l'accesso a una o più cartelle specifiche, con o senza cartelle secondarie. I livelli di accesso includono la visualizzazione, l'accesso, la modifica, l'eliminazione e la creazione (autorizzazioni aggiuntive). È possibile limitare l'accesso dell'utente a un ambiente specificato. Inoltre è possibile modificare l'accesso definito a gruppi predefiniti.

Per estendere l'accesso predefinito è necessario eseguire operazioni di personalizzazione. Ad esempio, la personalizzazione viene utilizzata per garantire agli amministratori l'accesso a CA EEM, creare diritti di accesso simili a quelli definiti nell'implementazione precedente di LDAP nonché limitare l'accesso ai server contenenti informazioni riservate o processi aziendali critici.

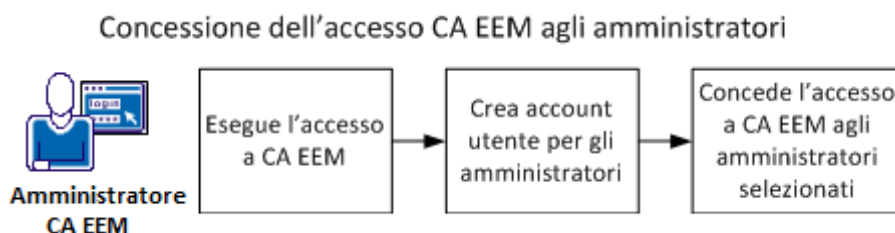
La sezione Riferimento alle autorizzazioni include le informazioni che consentono il supporto di tutti i tipi di personalizzazione.

Questa sezione contiene i seguenti argomenti:

# Concessione dell'accesso a CA EEM agli amministratori

CA EEM consente di proteggere CA Process Automation. CA EEM gestisce le credenziali negli account utente che consentono agli utenti di accedere a CA Process Automation. CA EEM autentica gli utenti al momento dell'accesso e consente l'accesso se l'ID utente e la password vengono individuati in un account utente. Gli account utente vengono associati a gruppi. CA EEM autorizza gli utenti al momento dell'accesso in base alle assegnazioni dei relativi gruppi.

EiamAdmin è il nome utente predefinito dell'amministratore di CA EEM. L'amministratore di CA EEM è il ruolo che concede agli utenti l'accesso a CA Process Automation. Durante l'installazione di CA Process Automation, specificare una password per l'utente EiamAdmin. Solo gli utenti che conoscono la password EiamAdmin possono accedere a CA EEM. Si consiglia di far conoscere questa password solo a pochi utenti fidati.

L'utente EiamAdmin può definire una norma che concede ad amministratori selezionati di CA Process Automation la capacità di creare gruppi personalizzati, norme e account utente. Questo accesso è sufficiente ma è più limitato rispetto a quello di EiamAdmin. Di seguito è riportata la procedura:

1. Cercare CA EEM ed eseguire l'accesso (a pagina 45).
2. Creare account utente per amministratori (a pagina 55).
3. Concedere ad amministratori selezionati l'accesso a CA EEM (a pagina 75).

**Ulteriori informazioni:**

Concessione dell'accesso a CA EEM ad amministratori specifici (a pagina 75)

## Concessione dell'accesso a CA EEM ad amministratori specifici

L'accesso a CA EEM è necessario per gestire account utente, gruppi e policy. Per impostazione predefinita, è necessario conoscere la password EiamAdmin per accedere a CA EEM con l'applicazione impostata per CA Process Automation. In genere, a conoscere questa password è un gruppo estremamente limitato poiché l'utente di EiamAdmin ha il controllo completo di CA EEM. Tuttavia, l'utente di EiamAdmin può concedere i diritti di accesso a CA EEM ad altri amministratori e può specificare gli oggetti che essi possono gestire. La procedura seguente mostra come consentire ad amministratori selezionati di gestire account utenti, gruppi e policy. La procedura comprende la definizione di un nuovo gruppo, la creazione di una policy personalizzata per tale gruppo e l'assegnazione del gruppo agli account utente.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Creare un gruppo di amministratori di CA EEM denominato EEMAdmins, i cui membri possono creare account utente, gruppi personalizzati e policy personalizzate.
    a. Fare clic sulla scheda Gestione identità.
    b. Fare clic su Gruppi.
    c. Fare clic su Nuovo gruppo applicazione.
    d. Immettere un nome per il gruppo (ad esempio, EEMAdmins).
    e. (Facoltativo) Aggiungere una descrizione.
    f. Fare clic su Salva.

    **Nota:** Non selezionare un gruppo applicazione.

3. Creare una policy che consenta di creare account utente, gruppi personalizzati e policy personalizzate. Assegnare EEMAdmins come identità per questa policy.

   a. Fare clic sulla scheda Gestione criteri di accesso.

   b. Fare clic su Criteri di ambito.

   c. Fare clic sul collegamento Administer Objects (Amministrazione oggetti).

   d. Fare clic su Salva con nome e immettere un nome per la policy (ad esempio Amministrazione di utenti e Policy).

   e. Fare clic su OK.

   f. Selezionare [User] EiamAdmin e [User] CERT-application-name dall'elenco Identità selezionate, quindi fare clic su Elimina.

   g. Fare clic su Cerca identità per il tipo Gruppo, quindi fare clic su Cerca.

   h. Selezionare il nuovo gruppo (EEMAdmins) e fare clic sulla freccia destra per spostare il gruppo utenti (ug) in Identità selezionate.

   i. Selezionare ed eliminare tutte le risorse *ad eccezione* di ApplicationInstance, Policy, User, UserGroup, GlobalUser, GlobalUserGroup, and Folder.

   j. Verificare che siano selezionate le azioni di lettura e scrittura.

   k. Fare clic su Salva.

   La policy è analoga all'esempio seguente:

**Criteri di ambito**

| Nome/Descrizione | ResourceClassName | Opzioni | Identità | Azioni | Risorse |
|---|---|---|---|---|---|
| Administrater Users and Policies<br>System Default: administrative access for the installer and the application instance certificate | SafeObject | Concessione esplicita | ug:EEMAdmins | read<br>write | ApplicationInstance<br>Policy<br>User<br>UserGroup<br>GlobalUser<br>GlobalUserGroup<br>Folder |

4. Aggiungere il gruppo EEMAdmins agli account utente degli amministratori selezionati.

   a. Fare clic sulla scheda Gestione identità.

   b. Fare clic su Informazioni su utente applicazione per cercare gli utenti.

   c. Selezionare Appartenenza gruppo come attributo, UGUALE A come operatore e PAMAdmins come valore.

   d. Fare clic su Vai.

      Gli amministratori di CA Process Automation vengono elencati.

   e. Fare clic sul nome di un amministratore.

      Viene visualizzato l'account utente dell'amministratore selezionato. EEMAdmins viene visualizzato come gruppo utenti disponibile.

   f. Fare clic sulla freccia destra per spostare EEMAdmins in Gruppi utenti selezionato.

   g. Fare clic su Salva.

5. Ripetere il passaggio 4 per tutti gli amministratori a cui si desidera concedere i privilegi di CA EEM.

## Personalizzazione dell'accesso utenti con le norme CA EEM

È possibile personalizzare l'accesso degli utenti a riquadri e schede di CA Process Automation e l'accesso ai diversi oggetti di automazione. Per estendere le modifiche a tutti i membri di un gruppo predefinito è possibile modificare le norme predefinite.

È possibile limitare l'accesso degli utenti a cartelle specifiche. Ad esempio è possibile creare una cartella per ciascun responsabile di progettazione e limitare l'accesso dei responsabili di progettazione alla propria cartella e alle cartelle progettate per un utilizzo comune.

È possibile limitare l'accesso di determinati utenti a un ambiente specifico. Ad esempio è possibile limitare l'accesso a un ambiente per i membri del gruppo Utenti dell'ambiente di produzione, in modo che possano accedere solo all'ambiente di produzione. In questo modo non potranno accedere all'ambiente di progettazione.

È possibile limitare l'accesso ai touchpoint che eseguono il mapping sui server che contengono informazioni sensibili o eseguire una funzionalità aziendale critica con le norme Protezione touchpoint.

## Controllo delle cache per gli aggiornamenti di CA EEM

CA Process Automation non riporta immediatamente le modifiche apportate in CA EEM a policy, gruppi utente e account utente. CA Process Automation non sempre interroga direttamente CA EEM per le query di autorizzazione. CA EEM non invia a CA Process Automation le singole modifiche quando vengono apportate. CA Process Automation invece utilizza le cache seguenti:

- Una cache sul lato di CA EEM per le modifiche a policy, gruppi utente e account utente che CA EEM invia a CA Process Automation.

  L'impostazione Protezione nella scheda Configurazione permette di controllare la frequenza di aggiornamento della cache. È possibile aggiornare l'impostazione a livello di dominio o per un ambiente selezionato.

- Una cache secondaria sul lato di CA Process Automation per i risultati di query che CA EEM restituisce a CA Process Automation.

  Durante la convalida delle autorizzazioni utente, la funzione di protezione valuta prima la durata della cache secondaria.

  - Se la durata della cache è uguale o minore rispetto al valore configurato, la funzione di protezione utilizza i dati di autorizzazione nella cache.
  - Se la durata della cache è maggiore rispetto al valore configurato, la funzione di protezione invia una richiesta a CA EEM. La funzione di protezione aggiorna la cache secondaria con i risultati della query e reimposta la durata della cache su 0 secondi.

Durante il test di policy personalizzate con un utente di test, è possibile visualizzare i risultati non appena CA EEM invia le modifiche a CA Process Automation. Per aggiornare CA Process Automation con una maggiore frequenza, ridurre l'intervallo di aggiornamento. Per ottimizzare le prestazioni del prodotto al termine della fase di test, aumentare l'intervallo di aggiornamento della cache.

Poiché si utilizza la procedura seguente per modificare la frequenza di aggiornamento della cache sul lato di CA EEM, valutare l'applicazione di una frequenza di aggiornamento veloce solo nell'ambiente di progettazione. Eventualmente, modificare la validità massima della cache secondaria sul server che ospita l'orchestrator di destinazione per il test.

**Attenersi alla procedura seguente:**

1. Modificare la frequenza con cui CA Process Automation riceve gli aggiornamenti da CA EEM. Impostare l'intervallo standard a livello di dominio.

   a. Fare clic sulla scheda Configurazione.

      Il riquadro Browser di configurazione viene visualizzato con il dominio selezionato. Viene visualizzata la scheda Protezione.

   b. Fare clic su Blocca.

   c. Modificare l'impostazione Intervallo di aggiornamento della cache CA EEM (in secondi) come necessario, in base alla frequenza di aggiornamento di CA EEM.

      - In fase di test per l'impatto delle modifiche apportate in CA EEM, impostare l'intervallo di aggiornamento su **60** secondi.
      - Al termine del test, impostare l'intervallo di aggiornamento su **1800** secondi (valore predefinito).

   d. Fare clic su Salva.

   e. Selezionare Dominio e fare clic su Sblocca.

   f. Riavviare l'orchestrator di dominio.

      - Interrompere l'orchestrator (a pagina 196).
      - Avviare l'orchestrator (a pagina 197).

2. Modificare la frequenza con cui CA EEM invia le modifiche per l'autorizzazione a CA Process Automation per un ambiente selezionato.

   a. Fare clic sulla scheda Configurazione ed espandere Dominio nel riquadro Browser di configurazione.

   b. Selezionare l'ambiente di destinazione e fare clic su Blocca.

   c. Nella scheda Protezione, modificare l'impostazione Intervallo di aggiornamento della cache CA EEM (in secondi) come necessario, a seconda se è in esecuzione il test delle autorizzazioni utente.

      - In fase di test delle personalizzazioni, impostare l'intervallo di aggiornamento su **60** secondi.

      - Al termine del test, impostare l'intervallo di aggiornamento su **1800** secondi (valore predefinito).

   d. Fare clic su Salva.

   e. Selezionare l'ambiente e fare clic su Sblocca.

   f. Riavviare gli orchestrator nell'ambiente aggiornato.

      - Interrompere l'orchestrator (a pagina 196).

      - Avviare l'orchestrator (a pagina 197).

3. Modificare la validità massima (in secondi) della cache secondaria che contiene le autorizzazioni utente.

   **Nota:** Generalmente non è necessario modificare questo parametro interno.

   a. Accedere al server sul quale è configurato l'orchestrator di destinazione.

   b. Individuare la seguente cartella o directory:

      *install_dir*/server/c2o/.config/

   c. Aprire il file OasisConfig.properties.

   d. Aggiungere il parametro seguente, se non esiste:

      ```
      eem.cache.timeout
      ```

   e. Assegnare un valore (in secondi).

      L'impostazione di questo parametro su 0 disattiva la cache in modo che CA Process Automation richieda le autorizzazioni utente da CA EEM quando sono obbligatorie. Il prodotto utilizza l'impostazione predefinita (30) quando il parametro non è presente nel file OasisConfig.properties.

      ```
      eem.cache.timeout=30
      ```

   f. Salvare il file.

   g. Riavviare il servizio Orchestrator.

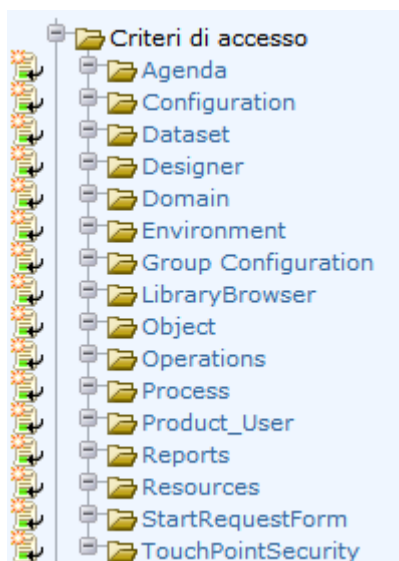
      - Interrompere l'orchestrator (a pagina 196).

      - Avviare l'orchestrator (a pagina 197).

**Ulteriori informazioni:**

Configurazione delle impostazioni di protezione di CA EEM per il dominio (a pagina 140)

## Classi di risorse predefinite e policy personalizzate

Le classi di risorse di CA Process Automation sono elencate nelle policy di accesso in CA EEM. È possibile creare una policy personalizzata originale per qualsiasi classe risorsa o basarla su una policy predefinita.

La maggior parte delle classi risorsa di CA EEM include policy predefinite.

È possibile utilizzare Salva con nome per salvare le policy di accesso predefinite con un nome nuovo, quindi personalizzarle in base alle proprie esigenze. La creazione di una policy personalizzata a partire da una policy predefinita consente di ottenere i risultati seguenti:

- Fornire al gruppo assegnato un'autorizzazione che la policy predefinita non concede. Ad esempio, una policy personalizzata può concedere al gruppo Responsabili di progettazione l'accesso al riquadro Installazione nella scheda Configurazione, per consentire loro di installare gli agenti.
- Rimuovere un'autorizzazione o un accesso che una policy predefinita concede. Ad esempio, la policy personalizzata può rimuovere i diritti di accesso del gruppo PAMUsers alla scheda Report.
- Sostituire un gruppo predefinito (ad esempio, PAMAdmins), con gruppi che rispecchiano meglio i ruoli del prodotto definiti dal sito. Ad esempio, è possibile avere tre livelli di amministrazione anziché uno. Assegnare PAMAdmins all'amministratore di dominio e creare gruppi di amministratori separati che gestiscono il contenuto ed eseguono le configurazioni per ciascun ambiente.

  **Nota:** Per ulteriori informazioni sulla creazione di diritti di accesso separati per gli amministratori del contenuto e gli amministratori della configurazione, consultare Creazione degli account utente con ruoli Active Directory personalizzati (a pagina 114).
- Aggiungere uno o più filtri per l'accesso specifico. Ad esempio, è possibile specificare come filtro AMBIENTE uguale a un nome ambiente. Il filtro di ambiente viene spesso utilizzato nelle policy di protezione del touchpoint definite dall'utente.

Valutare il processo e gli oggetti del modulo di richiesta di avvio in termini di chiamate del livello di accesso SOAP attraverso i servizi Web. Quando viene creata una policy con la classe di risorse Processo, i diritti di avvio (Process Start) o di controllo dei processi (Process_Control) vengono concessi agli utenti o ai gruppi specificati. Se l'utente che richiama il metodo di esecuzione del processo dispone dell'autorizzazione di avvio o controllo, il metodo viene eseguito correttamente. Quando viene creata una policy con la classe di risorse Modulo di richiesta di avvio, le autorizzazioni di avvio (StartRequestForm_Start) o di rimozione dalla coda (StartRequestForm_Dequeue) vengono concesse agli utenti o ai gruppi specificati. Se l'utente che esegue il metodo di esecuzione del modulo di richiesta di avvio dispone dell'autorizzazione di avvio o di rimozione dalla coda, il metodo viene eseguito correttamente. Se l'utente che esegue il metodo non dispone dei diritti di esecuzione per l'oggetto di destinazione, non è possibile eseguire correttamente il metodo. Il set di dati dell'operatore SOAP registra i messaggi di errore del metodo.

È possibile creare una policy personalizzata di CA EEM per concedere o negare l'accesso di gruppi specifici all'oggetto di automazione specificato. Ad esempio:

- Limitazione dell'accesso a un ambiente specificato mediante le policy Agenda, Set di dati, Sistema, Processo, Risorse, Modulo di richiesta di avvio, Protezione touchpoint. Aggiungere un filtro in cui Ambiente è l'attributo denominato e il nome dell'ambiente è il valore. L'operatore STRING è EQUAL ==. Nel seguente esempio di filtro, Test è il nome dell'ambiente:

- Limitare l'accesso a una cartella o a un oggetto specifico con la policy Oggetto. Aggiungere una risorsa, ad esempio /*folder_name* o /*folder_name*/*object_name*. Nell'esempio seguente, /folder_name rappresenta il nome della cartella in cui si trova l'oggetto di automazione.

È inoltre possibile creare una policy personalizzata per la classe di risorse Oggetto. Le policy relative all'oggetto forniscono un filtro che consente di specificare il tipo di oggetto al quale si applica la policy. Aggiungere un filtro in cui l'attributo denominato è Tipo di oggetto e il valore è un tipo di oggetto. L'operatore STRING è EQUAL ==. Nel seguente esempio di filtro, Risorse è il nome di Tipo di oggetto:

Altri valori validi includono:

- Classi di risorsa:
  - Agenda (classe risorsa per la pianificazione)
  - Set di dati
  - Processo
  - Risorse
  - Modulo di richiesta di avvio
- Calendario
- Icona personalizzata
- Operatore personalizzato
- Cartella
- Modulo di richiesta interazione
- Visualizzazione processo

## Personalizzazione dell'accesso per un gruppo predefinito

È possibile personalizzare l'accesso di un gruppo predefinito nei seguenti modi:

- Aggiunta un'azione a un gruppo predefinito.
- Revoca di un'azione assegnata a un gruppo predefinito.

Qualsiasi modifica effettuata alle assegnazioni di un gruppo predefinito viene applicata a tutti gli utenti assegnati a tale gruppo.

Di seguito viene riportato il processo che consente di personalizzare l'accesso per un gruppo predefinito:

1. Verifica delle autorizzazioni per i gruppi predefiniti (a pagina 47).
2. Identificazione di un'autorizzazione richiesta da parte della propria organizzazione, di cui un determinato gruppo non dispone.
3. Definizione del l'azione e della policy che controllano tale accesso.
   - Se l'autorizzazione consente di accedere a una scheda o a un riquadro, consultare Autorizzazioni per scheda (a pagina 100).
   - Se l'autorizzazione è per un oggetto di automazione, consultare Autorizzazioni per gli oggetti di automazione (a pagina 106).
4. Creazione di una policy basata su una policy esistente (a pagina 85), in cui la policy esistente è una policy predefinita e preimpostata.
5. Concessione o revoca di un'azione per un gruppo predefinito (a pagina 85).

## Creazione di una norma personalizzata basata su una norma esistente

È possibile creare una norma personalizzata basata su una norma predefinita o su un'altra norma personalizzata.

CA Process Automation include una norma per la maggior parte delle classi di risorsa. È possibile modificare le norme predefinite direttamente, in quanto sono modificabili. Tuttavia non è disponibile una procedura semplice per ripristinare la norma originale. È possibile creare una procedura che consenta di conservare le norme predefinite per confrontare la versione modificata con l'originale e ripristinare quest ultima.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic su Gestione di norme di accesso.
3. Fare clic sul nome della norma di accesso da modificare.
4. Fare clic sul collegamento della norma nella tabella delle norme.
5. Fare clic su Salva come e inserire un nome personalizzato per la norma.
6. Fare clic su Salva.
7. Se la norma personalizzata deve sostituire una norma predefinita, aprire la norma predefinita e fare clic su Disabilita. Quindi fare clic su Salva.

**Nota:** la norma personalizzata è pronta per la personalizzazione.

## Concessione o revoca di un'azione per un gruppo predefinito

È possibile concedere un'azione nuova a un gruppo predefinito. È possibile revocare anche un'azione predefinita a un gruppo predefinito.

**Attenersi alla procedura seguente:**

1. Aprire la norma personalizzata creata a questo scopo.
2. Nella riga Responsabili di progettazione per Identità selezionate, selezionare o deselezionare l'azione identificata.

   **Nota:** consultare Esempio: consentire ai responsabili di progettazione di eseguire installazioni (a pagina 86).

3. Fare clic su Salva.

   La norma personalizzata viene applicata la volta successiva che CA EEM invia aggiornamenti a CA Process Automation.

## Esempio: consentire ai responsabili di progettazione di eseguire installazioni

Per impostazione predefinita, i responsabili di progettazione non dispongono dell'accesso al riquadro Installazione nella scheda Configurazione. È possibile concedere agli utenti nel gruppo dei responsabili di progettazione anche la capacità di installare gli agenti. Selezionare Configuration_Installations (Installazioni) per responsabili di progettazione sulla policy di configurazione di PAM40.

## Esempio: Concessione del diritto di configurazione dei gruppi di operatori personalizzati ai responsabili di progettazione

Per impostazione predefinita, i responsabili di progettazione non possono effettuare le azioni seguenti sui gruppi di operatori personalizzati:

- Bloccare la configurazione del gruppo per un operatore personalizzato
- Definire un gruppo con variabili appropriate per un insieme di operatori personalizzati
- Sbloccare la configurazione del gruppo tramite la sua pubblicazione

I gruppi pubblicati di operatori personalizzati sono riportati nella scheda Moduli del browser di configurazione.

È possibile concedere ai responsabili di progettazione dei contenuti l'autorizzazione a creare e pubblicare gruppi di operatori personalizzati.

**Attenersi alla procedura seguente:**

1. Accedere a CA EEM.
2. Fare clic su Gestione delle policy di accesso.
3. Aprire la policy Configurazione del gruppo.
   a. Fare clic su Configurazione del gruppo.
   b. Fare clic sul collegamento della policy Configurazione del gruppo di PAM40.
4. Aggiungere il gruppo applicazione dei responsabili di progettazione all'elenco Identità selezionate.
   a. Selezionare Gruppo applicazione dall'elenco a discesa Tipo.
   b. Fare clic sull'opzione di ricerca delle identità.
   c. Accettare le voci predefinite per i campi seguenti, quindi fare clic su Cerca:
      - **Attributo:** Nome
      - **Operatore:** UGUALE A
      - **Valore**: il campo è vuoto per impostazione predefinita.
   d. Selezionare Progettazione e fare clic sulla freccia Giù:

5. Selezionare l'azione Group_Config_Admin per il gruppo dei responsabili di progettazione.

6. Fare clic su Salva.

## Limitazione dell'accesso in base all'ambiente

I gruppi predefiniti dei responsabili di progettazione e degli utenti dell'ambiente di produzione sono progettati per i casi tipici in cui sono presenti due ambienti:

- Ambiente di progettazione (ambiente predefinito)
- Ambiente di produzione (ambiente definito dall'utente)

I membri del gruppo di progettazione creano i processi aziendali automatizzati nell'ambiente di progettazione. I responsabili di progettazione, ad esempio, progettano i processi, i moduli di richiesta interazione e i set di dati.

I membri del gruppo degli utenti dell'ambiente di produzione utilizzano i processi progettati, i moduli progettati e i set di dati progettati. Ad esempio, gli utenti dell'ambiente di produzione avviano i processi, esaminano i set di dati e rispondono a richieste di interazione.

È possibile salvare le norme seguenti come norme personalizzate, per limitare l'accesso del gruppo dei responsabili di progettazione all'ambiente di progettazione e degli utenti dell'ambiente di produzione all'ambiente di produzione.

- agenda
- Set di dati
- Processo
- Risorse
- Modulo di richiesta di avvio

### Esempio: filtro Environment

È possibile limitare l'accesso alle pianificazioni per ambiente. Ad esempio è possibile utilizzare l'ambiente predefinito per la progettazione e aggiungere un ambiente di produzione per l'utilizzo dei processi e degli oggetti correlati che sono stati trasferiti alla produzione.

Il seguente filtro di esempio per le pianificazioni limita i membri del gruppo dei responsabili di progettazione all'ambiente predefinito. Limita i membri del gruppo degli utenti dell'ambiente di produzione all'ambiente di produzione.

| Nome/Descrizione | ResourceClassName | Filtri |
|---|---|---|
| Custom Schedule Policy with Environment Restrictions<br>Restrict Schedule automation object for Designer group to Default Environment and Production User group to Production Environment | Agenda | DOVE (( ug:Name == val:Designers<br>E req:action {} val:Agenda_Control<br>E name:ENVIRONMENT == val:Default Environment )<br>O ( ug:Name == val:Production Users<br>E req:action {} val:Control<br>E name:ENVIRONMENT == val:Production Environment )) |

È possibile personalizzare le norme in base alle seguenti norme predefinite, con filtri simili:

- Norma Set di dati di PAM40
- Norma Processo di PAM40
- Norma Modulo di richiesta di avvio di PAM40
- Norma Risorse di PAM40

Aprire la norma predefinita. Salvarla come norma personalizzata. Modificare il tipo in Norma di accesso. Quindi aggiungere il filtro.

## Personalizzazione dell'accesso con un gruppo personalizzato

Di seguito viene presentata la procedura di base per personalizzare l'accesso con un gruppo personalizzato:

1. Creare un gruppo personalizzato (a pagina 90).
2. Aggiungere un gruppo personalizzato a una norma predefinita (a pagina 91).

   Qui è possibile concedere autorizzazioni per azioni specifiche al gruppo personalizzato.

3. Assegnare il gruppo personalizzato ad account utente (a pagina 92).

   È possibile assegnare più di un gruppo a un account utente per estendere le autorizzazioni per tale utente.

**Nota:** per esempi di questa procedura, consultare Transizione dei ruoli utilizzati in Active Directory a CA EEM (a pagina 114).

## Creazione di un gruppo personalizzato

È possibile creare un gruppo di utenti di applicazioni personalizzato in CA EEM. Per concedere diritti a tale gruppo, aggiungere il gruppo alle policy e selezionare le azioni adeguate. Infine, assegnare il gruppo a singoli account utente.

**Nota:** le policy a cui è necessario aggiungere un gruppo personalizzato variano a seconda se tale gruppo si basa su uno esistente.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestione identità.
3. Fare clic su Gruppi.
4. Nel pannello Gruppi, fare clic sul pulsante Nuovo gruppo applicazione accanto a Gruppi applicazione per creare un gruppo personalizzato.
5. Immettere un nome per il gruppo nel campo Nome.
6. (Facoltativo) Immettere una descrizione per il gruppo.
7. (Facoltativo) Nel gruppo di selezione Appartenenza gruppo applicazione, selezionare PAMUsers per includere le autorizzazioni per l'accesso di base. In questo caso, è possibile limitare le autorizzazioni da concedere al gruppo personalizzato. Non è necessario concedere le autorizzazioni date al gruppo PAMUsers.

   **Nota:** se si lascia vuota l'area Gruppo utenti selezionato, il gruppo personalizzato deve disporre delle autorizzazioni per l'accesso di base.
8. Fare clic su Salva.

   Il nuovo gruppo viene visualizzato come un'opzione del gruppo utenti dell'applicazione quando si definiscono nuovi utenti.
9. (Facoltativo) In Cerca gruppi, selezionare Mostra gruppi applicazione, quindi fare clic su Vai.

   Il nuovo gruppo viene visualizzato con altri gruppi (inclusi quelli predefiniti).
10. Fare clic su Chiudi.

**Ulteriori informazioni:**

Aggiunta di un gruppo personalizzato a una norma predefinita (a pagina 91)

## Aggiunta di un gruppo personalizzato a una norma predefinita

Un modo semplice per personalizzare i privilegi di accesso è creare gruppi personalizzati e aggiungerli alle norme predefinite selezionate. Con questo approccio, non si creano norme personalizzate. Si identificano le azioni o le autorizzazioni nelle norme predefinite necessarie alle persone che vengono assegnate al gruppo personalizzato.

**Attenersi alla procedura seguente:**

1. Cercare CA EEM ed eseguire l'accesso (a pagina 45).
2. Creare un gruppo personalizzato per gli utenti che devono eseguire lo stesso set di attività in CA Process Automation.
   a. Fare clic sulla scheda Gestisci identità.
   b. Fare clic su Gruppi.
   c. Fare clic su Nuovo gruppo applicazione.
   d. Immettere il nome del gruppo.
   e. Non aggiungere l'appartenenza a un gruppo di applicazioni.
   f. Fare clic su Salva.
3. Aprire la norma predefinita contente l'azione che si desidera concedere.
   a. Fare clic sulla scheda di gestione delle norme di accesso.
   b. Fare clic sul collegamento per la classe di risorse appropriata in Norme di accesso.
   c. Fare clic sul collegamento nella tabella delle norme per la norma da aggiornare.

      Viene visualizzata la norma selezionata.
4. Concedere un'autorizzazione selezionata al gruppo personalizzato.
   a. In Inserisci/cerca identità, selezionare Gruppo applicazione dall'elenco a discesa Tipo e fare clic su Cerca.
   b. Selezionare il gruppo personalizzato dall'elenco e fare clic sulla freccia GIÙ.
   c. Il gruppo personalizzato verrà visualizzato nell'elenco Identità selezionate.
   d. Selezionare la casella di controllo per ogni azione da concedere.
   e. Fare clic su Salva.

   Il gruppo personalizzato viene aggiunto alla norma selezionata.

## Assegnazione di un gruppo personalizzato ad account utente

È possibile assegnare un gruppo personalizzato (ruolo) a un account utente durante il processo di creazione di tale account utente. Oppure è possibile modificare un account utente esistente per aggiungere il nuovo gruppo utenti dell'applicazione.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestisci identità.
3. Creare o accedere all'account utente di destinazione.
   - Fare clic su Nuovo utente per aggiungere un account utente.
   - Per recuperare un account utente esistente utilizzare il riquadro di ricerca degli utenti.
4. Se si crea un nuovo account, immettere l'ID dell'account utente nel campo Nome, immettere i dettagli relativi all'utente sotto i dettagli dell'utente globale, inserire una password temporanea e selezionare Modifica password accesso successivo.
5. Fare clic su Aggiungi informazioni su utente applicazione.
6. Selezionare il gruppo personalizzato dai gruppi di utenti disponibili e fare clic su > per spostarlo nei gruppi di utenti selezionati.
7. Fare clic su Salva, quindi su Chiudi.
8. Ripetere l'azione per ciascun utente che deve ricevere le autorizzazioni al gruppo personalizzato.
9. Fare clic su Disconnetti.

## Personalizzazione dell'accesso per un utente specificato

È possibile limitare gli oggetti che un utente di CA Process Automation specificato può visualizzare e quali azioni può eseguire. Ad esempio, è possibile creare regole in CA EEM per consentire a un utente di visualizzare o utilizzare unicamente un'istanza di oggetto di automazione o un oggetto di automazione. Questo tipo di accesso è possibile solo quando i responsabili di progettazione dei contenuti utilizzano gli oggetti di libreria in cartelle di lavoro. In questo caso, le versioni di rilascio degli oggetti vengono copiate in una cartella specifica del rilascio per esportarla come pacchetto di contenuto.

**Attenersi alla procedura seguente:**

1. Configurare le cartelle specifiche per la progettazione (a pagina 94).
2. Creare un account utente senza assegnazione di gruppi (a pagina 94).
3. Aggiungere l'utente a policy predefinite selezionate (a pagina 96).
4. Creare una policy oggetto personalizzata con autorizzazioni di percorso (a pagina 98).
5. Creare una policy personalizzata per un tipo di oggetto specificato (a pagina 99).

**Nota:** Accedere a CA Process Automation come l'utente specificato e verificare che l'accesso sia corretto.

## Configurazione di cartelle specifiche per la progettazione

È possibile progettare la struttura delle cartelle secondo le proprie esigenze. Per l'accesso specifico, progettare la struttura in modo tale da poter specificare un percorso per gli oggetti di un tipo specifico nella policy per tale oggetto di automazione. Per limitare un utente (o gruppo) a tipi di oggetto specifici o a tipi di oggetto specifici in progetti specificati, installare una struttura della cartella che permetta una restrizione di questo tipo. Ad esempio, installare una cartella Operazione in corso con una cartella per ciascun responsabile di progettazione.

**WIP/designer1**

Ciascun responsabile di progettazione ha una cartella di lavoro separata. Ciascuna cartella del responsabile di progettazione contiene un insieme di cartelle, uno per ciascun tipo di oggetto di automazione su cui lavora il responsabile di progettazione. Una cartella per set di dati può includere set di dati per più progetti sviluppati da un singolo responsabile di progettazione.

**/project1/releaseVersion1**

Ciascun progetto dispone di una cartella specifica, con una sottocartella per ciascuna versione di rilascio. Quando una versione di rilascio di un processo è pronta per la transizione alla produzione, copiare gli oggetti dalle cartelle di lavoro alla cartella della versione di rilascio. La cartella della versione di rilascio è la cartella che il prodotto esporta come pacchetto di contenuto.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA Process Automation (a pagina 18).
2. Fare clic sulla scheda Libreria.
3. Selezionare la cartella principale, fare clic su Nuovo e selezionare Cartella.
4. Immettere un nome breve per la nuova cartella.
5. Se necessario, ripetere questi passaggi per creare la struttura della cartella richiesta.

## Creazione di un account utente senza assegnazione di gruppi

È possibile creare un account utente senza assegnazione del gruppo. Questa procedura fa parte del processo per la creazione di accessi dettagliati, in cui le autorizzazioni dell'utente vengono ridotte alla progettazione e alla verifica degli oggetti di un tipo particolare.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestisci identità.

3. Fare clic sull'icona accanto a Utenti nel relativo riquadro.

   Viene visualizzata la pagina Nuovo utente.

4. Immettere l'ID utente da assegnare all'account utente nel campo Nome.

   Si tratta del nome da immettere nel campo Nome utente all'accesso.

5. Immettere i dettagli dell'utente globale.

   a. Immettere il nome nei campi Nome e Cognome.

      La barra del titolo visualizza questi valori quando l'utente accede a CA Process Automation.

   b. Completare gli altri campi necessari nell'area Generale.

6. (Facoltativo) Completare il campo Appartenenza gruppo globale se si utilizza CA Process Automation con un altro prodotto di CA Technologies che utilizza CA EEM.

7. Immettere e verificare una password da associare all'account nell'area Autenticazione.

   Fornire agli utenti la password temporanea configurata perché possano modificare le proprie password.

8. (Facoltativo) Completare i campi restanti nella pagina Nuovo utente.

9. Fare clic su Salva, quindi su Chiudi.

10. Fare clic su Disconnetti.

**Ulteriori informazioni:**

Utilizzo di CA EEM per la modifica della password di CA Process Automation (a pagina 46)
Concessione dell'accesso a CA EEM ad amministratori specifici (a pagina 75)

## Aggiunta dell'utente a policy predefinite selezionate

È possibile concedere le autorizzazioni di CA Process Automation a un'identità dell'utente in uno dei modi seguenti:

- Assegnare un gruppo utenti all'account utente.
- Aggiungere l'account utente alle policy selezionate. In ciascuna policy, assegnare azioni selezionate all'identità dell'utente

Se si sta lavorando con una policy personalizzata e ruoli dell'utente specifici, si consiglia di concedere l'accesso di base assegnando il gruppo PAMUsers all'account utente e poi estendendo l'accesso mediante le assegnazioni delle azioni del criterio.

Se si preferisce concedere l'accesso con i soli criteri, iniziare fornendo l'accesso di base. Aggiungere il nome dell'account utente ai criteri e alle azioni seguenti:

- Policy Accesso utente di PAM40: Console-Login (Utente)
- Policy Ambiente PAM40: Environment_Library_User (Utente)
- Policy Browser di libreria PAM40: LibraryBrowser_User (Utente del browser della libreria)

È possibile concedere l'accesso specifico alla scheda Operazioni. È possibile limitare l'accesso dell'utente ad azioni specificate in tipi di oggetti specifici.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestione criteri di accesso.
3. Aggiungere l'utente alla policy Accesso utente PAM40.
   a. Fare clic sul collegamento Utente del prodotto in Criteri di accesso.
   b. Fare clic sul collegamento della policy Accesso utente PAM40 in Tabella criteri.
   c. Impostare Tipo su **Utente** e fare clic su Cerca identità.
   d. Fare clic su Cerca.
   e. Selezionare l'identificatore utente dall'elenco visualizzato e fare clic sulla freccia giù.
   f. Selezionare Console-Login (Utente) per l'utente aggiunto.
   g. Fare clic su Salva, quindi su Chiudi.

4. Aggiungere l'utente alla policy Ambiente PAM40.
    a. Fare clic sul collegamento per Ambiente in Criteri di accesso.
    b. Fare clic sul collegamento della policy Ambiente PAM40 in Tabella criteri.
    c. Impostare Tipo su **Utente** e fare clic su Cerca identità.
    d. Fare clic su Cerca.
    e. Selezionare l'identificatore utente dall'elenco visualizzato e fare clic sulla freccia giù.
    f. Selezionare Environment_Library_User (Utente) per l'utente aggiunto.
    g. Fare clic su Salva, quindi su Chiudi.
5. Aggiungere l'utente alla policy Browser di libreria PAM40.
    a. Fare clic sul collegamento per Browser di libreria in Criteri di accesso.
    b. Fare clic sul collegamento della policy Browser di libreria PAM40 in Tabella criteri.
    c. Impostare Tipo su **Utente** e fare clic su Cerca identità.
    d. Fare clic su Cerca.
    e. Selezionare l'identificatore utente dall'elenco visualizzato e fare clic sulla freccia giù.
    f. Selezionare LibraryBrowser_User (Utente del browser di libreria) per l'utente aggiunto.
    g. Fare clic su Salva, quindi su Chiudi.
6. Concedere l'accesso dell'utente a due oggetti nella scheda Operazioni. Aggiungere l'utente alla policy Operazioni di PAM40 e specificare solo due azioni.
    a. Fare clic sul collegamento per Operazioni in Criteri di accesso.
    b. Fare clic sul collegamento della policy Operazioni PAM40 in Tabella criteri.
    c. Impostare Tipo su **Utente** e fare clic su Cerca identità.
    d. Fare clic su Cerca.
    e. Selezionare l'identificatore utente dall'elenco visualizzato e fare clic sulla freccia giù.
    f. Selezionare Operations_Datasets (Set di dati) per l'utente aggiunto.
    g. Selezionare Operations_Resources (Risorse) per l'utente aggiunto.
    h. Fare clic su Salva, quindi su Chiudi.

## Creazione di una norma oggetto personalizzata con autorizzazioni di percorso

Creare una norma di accesso oggetto personalizzata con la norma di accesso all'oggetto. Il numero di voci create dipende dalla lunghezza del percorso. Immettere una riga per ciascun livello del percorso, iniziando con la cartella principale (/).

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda di gestione delle norme di accesso.
3. Creare un norma oggetto personalizzata per limitare l'accesso di un utente specifico a un percorso specifico nella libreria.
   a. Fare clic sul collegamento Nuova norma di accesso per l'oggetto nelle norme di accesso.
   b. Immettere un nome.
   c. Selezionare Elenco controllo accesso per Tipo e fare clic su OK alla comparsa del messaggio di verifica.
   d. Fare clic su Cerca identità con l'opzione Tipo impostata su Utente.
   e. Fare clic su Cerca. Selezionare l'identificatore utente dall'elenco visualizzato e fare clic sulla freccia destra.
   f. Immettere una barra in avanti (/) nel campo Aggiungi risorsa e fare clic su Aggiungi.
   g. Nello stesso campo, digitare il simbolo / seguito dal nome della cartella contenente gli oggetti a cui l'utente viene limitato. Fare clic su Aggiungi.
   h. Selezionare Object_List (Elenco) per la cartella principale (/).
   i. Selezionare Object_List (Elenco) per il percorso /*cartella.* Ripetere questa passaggio se esiste un percorso *cartella*/*cartella secondaria.*

      Nota: è possibile immettere /cartella/cartella secondaria* e selezionare Tratta i nomi risorse come espressioni regolari per includere tutte le cartelle subordinate nella cartella secondaria specificata.
   j. Fare clic su Salva. Fare clic su Chiudi.

## Creazione di una norma personalizzata per un tipo di oggetto specificato

Creare una norma per il tipo di oggetto per cui è valida la restrizione. Quindi specificare le azioni da autorizzare sul tipo di oggetto selezionato. Scegliere tra i tipi di norme seguenti:

- agenda
- Set di dati
- Processo
- Risorse
- Modulo di richiesta di avvio

**Nota:** per informazioni sulle autorizzazioni, consultare la sezione Guida di riferimento alle autorizzazioni (a pagina 100).

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda di gestione delle norme di accesso.
3. Creare una norma personalizzata per il tipo di oggetto al quale si desidera limitare l'accesso.
   a. Fare clic sul collegamento Nuova norma di accesso per uno dei seguenti tipi di risorse: Agenda, Set di dati, Processo, Risorse, Modulo di richiesta di avvio.
   b. Immettere un nome.
   c. Selezionare Elenco controllo accesso per Tipo e fare clic su OK alla comparsa del messaggio di verifica.
   d. Fare clic su Cerca identità con l'opzione Tipo impostata su Utente.
   e. Fare clic su Cerca. Selezionare l'identificatore utente dall'elenco visualizzato e fare clic sulla freccia destra.
   f. Nel campo Aggiungi risorsa, digitare il percorso completo, contenente il tipo di oggetto selezionato. Fare clic su Aggiungi.
   g. Nello stesso campo, digitare una barra in avanti (/), quindi digitare il nome della cartella contenente gli oggetti a cui l'utente viene limitato. Fare clic su Aggiungi.
   h. Selezionare le autorizzazioni da concedere.
      - Agenda: Agenda_Control (Controllo). L'agenda fa riferimento alle Pianificazioni.
      - Set di dati: Dataset_Inspect (Ispeziona), Dataset_Modify (modifica).
      - Processo: Process_Control (Controllo), Process_Monitor (Monitoraggio), Process_Start (Avvia).
      - Risorse: Resources_Control

i. Fare clic su Salva. Fare clic su Chiudi.

4. (Facoltativo) Aggiungere un filtro per porre dei limiti in base all'ambiente.
5. Ripetere questa procedura per gli oggetti dipendenti. Considerare, ad esempio, i Set di dati. I Set di dati sono significativi solamente nel contesto di un altro tipo di oggetto. Se sono stati selezionati i Set di dati, creare un'altra norma, ad esempio per le risorse.

# Guida di riferimento alle autorizzazioni

Le tabelle seguenti elencano tutte le autorizzazioni con dipendenze e filtri:


- Autorizzazioni per scheda (a pagina 100)
- Autorizzazioni per gli oggetti di automazione (a pagina 106)
- Dipendenze delle autorizzazioni (a pagina 109)
- Filtri per autorizzazioni (a pagina 112)


## Autorizzazioni per scheda

Le azioni selezionate a livello delle policy predefinite di CA EEM concedono le autorizzazioni di accesso a schede, riquadri, cartelle e oggetti di automazione. Le seguenti tabelle descrivono le autorizzazioni concesse da ogni azione ai gruppi (identità) nelle policy di risorsa corrispondenti.

Se si creano policy personalizzate da queste classi di risorsa, utilizzare le tabelle corrispondenti come guida per l'assegnazione delle autorizzazioni.

### Scheda Pagina iniziale

| Tasto di azione (Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Console_Login (Utente) | Utente del prodotto | Accedere a CA Process Automation e fare clic sulla scheda Pagina iniziale. |

### Scheda Libreria

Le autorizzazioni riportate nella tabella seguente vengono visualizzate in ordine crescente. Per visualizzare la scheda Libreria, è necessario disporre delle autorizzazioni LibraryBrowser_User ed Environment_Library_User o Environment_Library_Admin. Per ulteriori informazioni, consultare la sezione Dipendenze delle autorizzazioni (a pagina 109).

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| LibraryBrowser_User<br>(Utente del browser di libreria) | LibraryBrowser<br>(Browser di libreria) | Visualizzare l'accesso alla scheda Libreria. |
| Object_List<br>(Elenco) | Oggetto | ■ Visualizzare la cartella o l'oggetto di automazione nella libreria.<br>■ Definire le visualizzazioni personalizzate della libreria. |
| Environment_Library_User<br>(Utente) | Ambiente | Prerequisito per numerose autorizzazioni nella scheda Operazioni.<br>■ Accesso agli orchestrator aggiunti agli ambienti.<br>■ Visualizzare, esportare, cercare oggetti di automazione nella scheda Libreria se l'accesso è impostato. |
| Object_Read<br>(Lettura) | Oggetto | Accedere al percorso di una cartella e aprire qualsiasi oggetto di automazione nella finestra di progettazione o nel visualizzatore corrispondente.<br>*Implicito:* Elenco |
| Object_Edit<br>(Modifica) | Oggetto | Modificare una cartella o un oggetto di automazione in una cartella.<br>*Implicito:* Lettura, Elenco |
| Object_Delete<br>(Elimina) | Oggetto | Eliminare una cartella o un oggetto di automazione aggiunti a una cartella.<br>*Implicito:* Modifica, Lettura, Elenco |
| Object_Admin<br>(Amministratore) | Oggetto | Creare una cartella o qualsiasi oggetto di automazione.<br>*Implicito:* Elimina, Modifica, Lettura, Elenco |
| Environment_Library_Admin<br>(Amministratore del contenuto) | Ambiente | Creare, eliminare, modificare, leggere ed elencare tutti gli oggetti di automazione contenuti nella scheda Libreria. |

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Group_Config_Admin | Configurazione del gruppo | Accedere alla scheda Configurazione del gruppo. Per informazioni sulle autorizzazioni relative agli operatori personalizzati, consultare la sezione Autorizzazioni per gli oggetti di automazione (a pagina 106). |

### Scheda Progettazione

Generalmente, gli utenti con accesso alla scheda Progettazione dispongono anche delle autorizzazioni di accesso alla scheda Libreria. I responsabili di progettazione devono disporre almeno delle seguenti autorizzazioni sulla scheda Libreria per salvare un processo in corso di progettazione:

- LibraryBrowser_User
- Environment_Library_User
- Object_Edit (che comprende le autorizzazioni Object_List e Object_Read)

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Designer_User<br>(Utente di progettazione) | Progettazione | Visualizzare l'accesso alla scheda Progettazione. |

### Riquadri e scheda Operazioni

I responsabili di progettazione devono disporre dell'accesso alla scheda Operazioni nell'ambiente di progettazione, mentre gli utenti dell'ambiente di produzione devono disporre dell'accesso alla scheda Operazioni nell'ambiente di produzione. Per visualizzare la scheda Operazioni, è necessario disporre dell'autorizzazione Environment_Library_User o Environment_Library_Admin. Per ulteriori informazioni, consultare la sezione Dipendenze delle autorizzazioni (a pagina 109).

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Operations_Process_Watch<br>(Visualizzazione processo) | Operazioni | ■ Aprire il riquadro Visualizzazione processo nella scheda Operazioni.<br>■ Visualizzare tutti i processi con lo stato selezionato, le pianificazioni attive, gli operatori attivi e le Richieste utente. |

| **Tasto di azione<br>(Nome localizzato)** | **Classe risorsa per la policy** | **Autorizzazioni** |
|---|---|---|
| Process_Monitor<br>(Monitoraggio) | Processo | ■ Aprire un'istanza di processo in esecuzione nella Progettazione processi.<br>■ Monitorare l'avanzamento.<br>■ Impostare i punti di interruzione.<br>*Implicito:* Elenco |
| Process_Start<br>(Avvia) | Processo | Avviare un'istanza di processo.<br>*Implicito:* Monitora, Elenco |
| Process_Control<br>(Controllo) | Processo | Sospendere, riavviare, riprendere o interrompere le istanze di processo.<br>*Implicito:* Avvia, Monitora, Elenco |
| Operations_Schedules<br>(Pianificazioni) | Operazioni | Visualizzare il collegamento Pianificazioni attive nella scheda Operazioni. |
| Agenda_Control<br>(Controllo) | agenda | Attivare e disattivare una pianificazione su un touchpoint.<br>*Implicito:* Lettura, Elenco |
| Operations_Datasets<br>(Set di dati) | Operazioni | Aprire il riquadro Set di dati nella scheda Operazioni. |
| Dataset_Inspect<br>(Ispeziona) | Set di dati | Visualizzare un oggetto del set di dati e leggere i valori delle variabili nel set di dati.<br>*Implicito:* Elenco |
| Dataset_Modify<br>(Modifica) | Set di dati | Creare, modificare ed eliminare l'oggetto del set di dati.<br>*Implicito:* Controlla, Lettura, Elenco |
| Operations_Resources<br>(Risorse) | Operazioni | Aprire il riquadro Risorse nella scheda Operazioni. |
| Resources_Control<br>(Controllo) | Risorse | ■ Bloccare, sbloccare, acquisire, restituire o aggiungere un parametro a una risorsa.<br>■ Aggiungere o rimuovere un'unità di risorsa.<br>*Implicito*: Lettura, Elenco |
| Operations_User_Requests<br>(Richieste utente) | Operazioni | Aprire il riquadro Richieste utente nella scheda Operazioni. |
| Operations_Content_Packages (Pacchetti di contenuto) | Operazioni | Aprire il riquadro Pacchetti di contenuto nella scheda Operazioni. |

| **Tasto di azione (Nome localizzato)** | **Classe risorsa per la policy** | **Autorizzazioni** |
|---|---|---|
| Operations_Task_List (Elenco attività) | Operazioni | ■ Utilizzare il collegamento Elenco attività nella scheda Operazioni e visualizzare le attività dell'utente, del gruppo utente o di qualsiasi gruppo.<br>■ Accedere alle attività dalla scheda Pagina iniziale. |
| StartRequestForm_Dequeue (Rimuovi dalla coda) | Modulo di richiesta di avvio | Rimuovere dalla coda un processo messo in coda da un Modulo di richiesta di avvio.<br>*Implicito*: Avvia, *E*lenco |
| StartRequestForm_Start (Avvia) | Modulo di richiesta di avvio | Avviare un'attività definita da un modulo di richiesta di avvio.<br>*Implicito:* Elenco |
| Esegui | Protezione touchpoint | Eseguire script o programmi negli operatori. Il prodotto trae gli operatori interessati da categorie di operatore specifiche. L'impatto si produce quando la destinazione è costituita da un determinato touchpoint in un ambiente specificato. |

### Scheda Report

Nella tabella seguente vengono riportate le azioni relative all'uso della scheda Report.

| **Tasto di azione (Nome localizzato)** | **Classe risorsa per la policy** | **Autorizzazioni** |
|---|---|---|
| Reports_User (Utente report) | Report | ■ Aprire la scheda Report<br>■ Caricare report personalizzati<br>■ Visualizzare o eliminare report predefiniti, condivisi o privati. |

### Riquadri e scheda di configurazione

Nella tabella seguente vengono riportate le azioni che influiscono sulle autorizzazioni nella scheda Configurazione. Per visualizzare il browser di configurazione nella scheda Configurazione, è necessario disporre dell'autorizzazione Client_Configuration_User. Per ulteriori informazioni, consultare la sezione Dipendenze delle autorizzazioni (a pagina 109).

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Client_Configuration_User<br>(Visualizza Browser di configurazione) | Browser di configurazione | Visualizzare il browser di configurazione nella scheda Configurazione. |
| Environment_Configuration_Admin<br>(Amministratore della configurazione) | Ambiente | ■ Aggiungi nuovo gruppo, Aggiungi touchpoint e Aggiungi gruppo host nel browser di configurazione.<br>■ Modificare la configurazione a livello di ambiente, inclusi protezione, proprietà, categorie operatori, gruppi di operatori personalizzati e trigger. |
| Domain_Admin<br>(Amministratore) | Dominio | ■ Nel riquadro Browser di configurazione, bloccare o sbloccare il dominio, aggiungere l'ambiente, richiamare Rimozione agente in blocco e Rimozione touchpoint in blocco.<br>■ Modificare la configurazione a livello di dominio, inclusi protezione, proprietà, categorie operatori, gruppi di operatori personalizzati e trigger.<br>■ Aggiornare i contenuti della cartella Risorse orchestrator e Risorse agente nel riquadro Gestisci risorse utente. |
| Configuration_User_Resources<br>(Risorse utente) | Browser di configurazione | Aprire il riquadro Gestisci risorse utente della scheda Configurazione e aggiornare i contenuti della cartella Risorse utente. |
| Configuration_Installations<br>(Installazioni) | Browser di configurazione | Aprire il riquadro Installazione della scheda Configurazione e installare un agente, un orchestrator o il nodo cluster di un orchestrator. |

**Ulteriori informazioni:**

Dipendenze delle autorizzazioni (a pagina 109)

## Autorizzazioni per gli oggetti di automazione

La tabella seguente descrive le autorizzazioni che è possibile concedere per diversi oggetti di automazione tramite policy personalizzate di CA EEM. È possibile concedere le autorizzazioni a qualsiasi gruppo applicazioni in CA EEM. Per poter accedere a cartelle e oggetti di automazione su qualsiasi orchestrator in un ambiente è necessario che l'utente o l'amministratore del contenuto esegua l'accesso nella policy Ambiente. L'ambiente è la classe di risorse padre per le classi di risorse degli oggetti di automazione.

Alcune autorizzazioni includono in modo implicito altre autorizzazioni. Quando si seleziona un'autorizzazione specifica, vengono selezionate contemporaneamente autorizzazioni implicite. Quando si concede un'autorizzazione esplicita, implicitamente si concedono tutte le altre autorizzazioni sotto di essa nella gerarchia di autorizzazione.

Quando si nega un'autorizzazione implicita, si negano tutte le altre autorizzazioni al di sopra di essa nella gerarchia di autorizzazione. L'autorizzazione Elenco è implicita in ogni altra autorizzazione e non dipende da altre autorizzazioni. È possibile negare a un gruppo tutte le autorizzazioni per una cartella mediante una policy personalizzata Oggetto che nega le autorizzazioni con Elenco. La revoca dell'autorizzazione Elenco revoca ogni altra autorizzazione per un oggetto di automazione. Tuttavia, la revoca di altre autorizzazioni non comporta mai la revoca dell'autorizzazione Elenco.

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Object_Admin<br>(Amministratore) | Oggetto | Creare una cartella o qualsiasi oggetto di automazione<br>**Implicito:** Elimina, Modifica, Lettura, Elenco |
| Object_Delete<br>(Elimina) | Oggetto | Eliminare una cartella o un oggetto di automazione aggiunti a una cartella.<br>**Implicito:** Modifica, Lettura, Elenco |
| Object_Edit<br>(Modifica) | Oggetto | Modificare una cartella o un oggetto di automazione in una cartella.<br>**Implicito**: Lettura, Elenco |
| Object_Read<br>(Lettura) | Oggetto | Accedere al percorso di una cartella e aprire qualsiasi oggetto di automazione nella finestra di progettazione o nel visualizzatore corrispondente.<br>**Implicito:** Elenco |
| Object_List<br>(Elenco) | Oggetto | Visualizzare una cartella o un oggetto di automazione nel browser di libreria. Definire visualizzazioni personalizzate della libreria. |

| Tasto di azione (Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Environment_Library_Admin (Amministratore del contenuto) | Ambiente | Creare, eliminare, modificare, leggere, elencare tutti gli oggetti di automazione |
| Environment_Library_User (Utente) | Ambiente | Visualizzare, esportare e cercare oggetti di automazione (se l'accesso è impostato).<br>**Nota**: ereditarietà implicita da classi di risorse per gli oggetti di automazione |
| Agenda_Control (Controllo) | agenda | Attivare e disattivare una pianificazione su un touchpoint.<br>**Implicito**: Lettura, Elenco |
| Dataset_Modify (Modifica) | Set di dati | Creare, modificare ed eliminare l'oggetto del set di dati.<br>**Implicito:** Controlla, Lettura, Elenco |
| Dataset_Inspect (Ispeziona) | Set di dati | Visualizzare un oggetto di set di dati e leggere i valori di variabili nel set di dati.<br>**Implicito:** Elenco |
| Process_Control (Controllo) | Processo | Sospendere, riavviare, riprendere o interrompere le istanze di un processo.<br>**Implicito:** Avvia, Monitora, Elenco |
| Process_Start (Avvia) | Processo | Avviare un'istanza di processo.<br>**Implicito:** Monitora, Elenco |
| Process_Monitor (Monitoraggio) | Processo | Aprire un'istanza in esecuzione di un processo in Progettazione processi, monitorare l'avanzamento e impostare i punti di interruzione.<br>**Implicito:** Elenco |
| Resources_Control (Controllo) | Risorse | Bloccare, sbloccare, acquisire, restituire o aggiungere un parametro a una risorsa. Aggiungere o rimuovere un'unità di risorsa.<br>**Implicito**: Lettura, Elenco |
| StartRequestForm_Dequeue (Rimuovi dalla coda) | Modulo di richiesta di avvio | Rimuovere dalla coda un processo inserito in tale coda da un Modulo di richiesta di avvio.<br>**Implicito**: Avvia, *E*lenco |
| StartRequestForm_Start (Avvia) | Modulo di richiesta di avvio | Avviare un'attività definita da un Modulo di richiesta di avvio.<br>**Implicito:** Elenco |

| Tasto di azione (Nome localizzato) | Classe risorsa per la policy | Autorizzazioni |
|---|---|---|
| Esegui | Protezione touchpoint | Eseguire script o programmi in operatori derivati dalle categorie di operatori specificate che utilizzano come destinazione touchpoint specifici in un ambiente determinato. |
| Group_Config_Admin | Configurazione del gruppo | Definire parametri per un gruppo di operatori personalizzati tramite la definizione dell'operatore personalizzato.<br>**Attenersi alla procedura seguente:**<br>1. Bloccare il gruppo di operatori personalizzati nella scheda Configurazione del gruppo.<br>2. Aggiungere pagine e variabili.<br>3. Salvare la configurazione.<br>4. Sbloccare il gruppo di operatori personalizzati,<br>in modo da pubblicare la configurazione del gruppo di operatori personalizzati definito. La pubblicazione rende la configurazione del gruppo disponibile nella scheda Moduli del browser di configurazione a livello di dominio e di ambiente. |

**Ulteriori informazioni:**

Dipendenze delle autorizzazioni (a pagina 109)

## Dipendenze delle autorizzazioni

La tabella seguente descrive l'azione della classe di risorsa dipendente (autorizzazione) per ciascuna azione della classe di risorsa nelle policy predefinite di CA EEM per CA Process Automation.

Valutare le dipendenze quando agli account utente si assegnano solo gruppi personalizzati (senza PAMUsers).

La tabella riportata di seguito contiene un riepilogo dei tasti di azione che è possibile assegnare in una policy personalizzata per una classe di risorsa a un gruppo personalizzato. Se si crea una policy personalizzata di questo tipo, assegnare il gruppo personalizzato a un tasto di azioni dipendenti.

| **Tasto di azione (Nome localizzato)** | **Classe risorsa per la policy personalizzata** | **Tasto delle azioni dipendenti (Nome localizzato)** |
|---|---|---|
| Console_Login (utente) | Utente del prodotto | |
| Reports_User (Utente report) | Report | Console_Login (utente) |
| Environment_Library_User (utente) | Ambiente | Console_Login (utente) |
| Environment_Library_Admin (amministratore contenuto) | Ambiente | Console_Login (utente) |
| Environment_Configuration_Admin (amministratore configurazione) | Ambiente | Console_Login (utente) |
| Domain_Admin (amministratore) | Dominio | Console_Login (utente) |
| Client_Configuration_User (Visualizza Browser di configurazione) | Browser di configurazione | Console_Login (utente) |
| Configuration_User_Resources (Risorse utente) | Browser di configurazione | ■ Console_Login (utente)<br>■ Client_Configuration_User (Visualizza Browser di configurazione)<br>■ Domain_Admin (Amministratore) per accedere alle cartelle Risorse agente e Risorse orchestrator. |
| Configuration_Installations (Installazioni) | Browser di configurazione | Console_Login (utente) |
| LibraryBrowser_User (Utente del browser di libreria) | Browser di libreria | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |

| Tasto di azione (Nome localizzato) | Classe risorsa per la policy personalizzata | Tasto delle azioni dipendenti (Nome localizzato) |
|---|---|---|
| Operations_User_Requests (Richieste utente) | Operazioni | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |
| Operations_Process_Watch (Visualizzazione processo) | Operazioni | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |
| Operations_Task_List (Elenco attività) | Operazioni | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |
| Operations_Schedules (Pianificazioni) | Operazioni | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |
| Operations_Resources (Risorse) | Operazioni | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |
| Operations_Datasets (Set di dati) | Operazioni | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |
| Operations_Content Packages (Pacchetti di contenuto) | Operazioni | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) o Environment_Library_Admin (amministratore del contenuto) |

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy personalizzata | Tasto delle azioni dipendenti<br>(Nome localizzato) |
|---|---|---|
| ■ Object_List (elenca)<br>■ Object_Read (leggi)<br>■ Object_Edit (modifica)<br>■ Object_Delete (elimina)<br>■ Object_Admin (Ammin.) | Oggetto | ■ Console_Login (utente)<br>■ Environment_Library_User (utente) |
| Agenda_Control (controlla) | agenda | ■ Console_Login (utente)<br>■ Environment_Library_User (utente)<br>■ Object_List (Elenco) con risorsa/*cartella*<br>**Nota:** se l'oggetto viene creato nella cartella principale, Object_List non è necessario. |
| ■ Dataset_Inspect (ispeziona)<br>■ Dataset_Modify (modifica) | Set di dati | ■ Console_Login (utente)<br>■ Environment_Library_User (utente)<br>■ Object_List (Elenco) con risorsa/*cartella*<br>**Nota:** se l'oggetto viene creato nella cartella principale, Object_List non è necessario. |
| ■ Process_Control (controlla)<br>■ Process_Monitor (monitora)<br>■ Process_Start (avvia) | Processo | ■ Console_Login (utente)<br>■ Environment_Library_User (utente)<br>■ Object_List (Elenco) con risorsa/*cartella*<br>**Nota:** se l'oggetto viene creato nella cartella principale, Object_List non è necessario. |
| Resources_Control (controlla) | Risorse | ■ Console_Login (utente)<br>■ Environment_Library_User (utente)<br>■ Object_List (Elenco) con risorsa/*cartella*<br>**Nota:** se l'oggetto viene creato nella cartella principale, Object_List non è necessario. |

| Tasto di azione<br>(Nome localizzato) | Classe risorsa per la policy personalizzata | Tasto delle azioni dipendenti<br>(Nome localizzato) |
|---|---|---|
| ■ StartRequestForm_Start (avvia)<br>■ StarRequestForm_Dequeue (Rimozione dalla coda) | Modulo di richiesta di avvio | ■ Console_Login (utente)<br>■ Environment_Library_User (utente)<br>■ Object_List (Elenco) con risorsa/*cartella*<br>**Nota:** se l'oggetto viene creato nella cartella principale, Object_List non è necessario. |
| Esegui | Protezione touchpoint | ■ Console_Login (utente)<br>■ Environment_Library_User (utente)<br>■ Object_List (Elenco) con risorsa/*cartella*<br>**Nota:** se l'oggetto viene creato nella cartella principale, Object_List non è necessario. |
| Group_Config_Admin | Configurazione del gruppo | ■ Console_Login (utente)<br>■ Environment_Library_User (utente)<br>■ Object_List (Elenco) con risorsa/*cartella*<br>■ Object_Edit (Modifica) con risorsa/*cartella* |

**Ulteriori informazioni:**

Autorizzazioni per gli oggetti di automazione (a pagina 106)
Autorizzazioni per scheda (a pagina 100)

## Filtri per autorizzazioni

CA EEM definisce le autorizzazioni come azioni di classe risorsa. Facoltativamente, è possibile utilizzare i filtri per limitare le azioni consentite a un gruppo o a un utente. Ad esempio, è possibile definire l'ambito delle autorizzazioni in modo che valgano solo per il gruppo assegnato nell'ambiente configurato.

L'esempio di Filtri seguente illustra l'impiego di AMBIENTE come attributo denominato per il filtro. Le policy definite con il tipo Criteri di accesso consentono di aggiungere dei filtri.

Le azioni contenute nella tabella seguente appartengono alle policy basate sulla classe risorsa di riferimento.

| Tasto di azione (Nome localizzato) | Classe risorsa per la policy | Attributo denominato per il filtro |
|---|---|---|
| Object_List (elenca)<br>Object_Read (leggi)<br>Object_Edit (modifica)<br>Object_Delete (elimina)<br>Object_Admin (Ammin.) | Oggetto | SECURITY_CONTEXT_ID<br>SECURITY_CONTEXT_GRP<br>ENVIRONMENT<br>OBJECT_TYPE |
| Agenda_Control (controlla) | agenda | ENVIRONMENT |
| Dataset_Inspect (ispeziona)<br>Dataset_Modify (modifica) | Set di dati | ENVIRONMENT |
| Process_Control (controlla)<br>Process_Monitor (monitora)<br>Process_Start (avvia) | Processo | SECURITY_CONTEXT_ID<br>SECURITY_CONTEXT_GRP<br>ENVIRONMENT |
| Resources_Control (controlla) | Risorse | ENVIRONMENT |
| StartRequestForm_Start (avvia)<br>StarRequestForm_Dequeue (Rimozione dalla coda) | Modulo di richiesta di avvio | ENVIRONMENT |
| Esegui | Protezione touchpoint | ENVIRONMENT<br>TOUCHPOINT |

# Transizione dei ruoli Active Directory a CA EEM

Se precedentemente si utilizzava Microsoft Active Directory (AD) o LDAP per l'autenticazione e l'autorizzazione, è possibile eseguire la transizione a CA EEM con uno dei due metodi seguenti:

- Creare un account utente. Assegnare uno dei gruppi predefiniti a ciascun account.

  **Nota:** consultare la sezione Verifica delle autorizzazioni per gruppi predefiniti (a pagina 47).

- Scegliere AD come archivio utenti esterno.

  **Nota:** consultare Gestione dell'accesso per account utente di riferimento (a pagina 61). Consultare Integrazione di Active Directory con CA EEM.

- Creare gruppi personalizzati che riflettono i propri ruoli di AD. Aggiungere questi gruppi alle policy di CA EEM e concedere le autorizzazioni necessarie. Creare un account utente. Assegnare uno dei gruppi personalizzati a ciascun account. Questa sezione illustra questo metodo.

Presupporre di aver definito le impostazioni di protezione del dominio in Active Directory con questi gruppi: ITPAMAdmins, ITPAMUsers, ConfigAdmin, ContentAdmin e EnvironmentUser.

**Impostazioni di protezione del dominio**

| | |
|---|---|
| Amministratore di dominio | ITPAMAdmins |
| Utente di CA IT PAM | ITPAMUsers |
| Amministratore della configurazione di ... | ConfigAdmin |
| Amministratore del contenuto di ambiente | ContentAdmin |
| Utente di ambiente | EnvironmentUser |

Per eseguire manualmente la migrazione dell'accesso basato su ruoli da Active Directory a CA EEM, utilizzare la procedura riportata di seguito.

**Attenersi alla procedura seguente:**

1. Eseguire la migrazione dell'accesso basato sui ruoli per gli utenti presenti nel ruolo Amministratore di dominio.

   Consultare la sezione Creazione degli account utente per gli amministratori (a pagina 55).

2. Eseguire la migrazione dell'accesso basato sui ruoli per gli utenti presenti nel ruolo Utente CA Process Automation.

   Consultare la sezione Creazione di account utente con accesso di base (a pagina 58).

3. Eseguire la migrazione dell'accesso basato sui ruoli per gli utenti presenti nel ruolo di Amministratore della configurazione di ambiente come indicato di seguito:

   a. Creare il gruppo ConfigAdmin personalizzato (a pagina 115).

   b. Concedere le autorizzazioni al gruppo ConfigAdmin personalizzato (a pagina 116).

   c. Creare account utente per gli amministratori della configurazione di ambiente (a pagina 117).

4. Eseguire la migrazione dell'accesso basato sui ruoli per gli utenti presenti nel ruolo di Amministratore del contenuto di ambiente come indicato di seguito:

   a. Creare il gruppo ContentAdmin personalizzato (a pagina 118).

   b. Concedere le autorizzazioni al gruppo ContentAdmin personalizzato (a pagina 119).

   c. Creare account utente per gli amministratori del contenuto di ambiente (a pagina 120).

5. Eseguire la migrazione dell'accesso basato sui ruoli per gli utenti presenti nel ruolo Utente di ambiente.

   Consultare la sezione Creazione di account utente per utenti dell'ambiente di produzione (a pagina 57).

## Creazione del gruppo ConfigAdmin personalizzato

È possibile creare un gruppo personalizzato ConfigAdmin per gli utenti presenti nel ruolo Amministratore della configurazione di ambiente.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).

2. Fare clic sulla scheda Gestione identità, selezionare Gruppi, quindi Nuovo gruppo applicazioni.

3. Digitare **ConfigAdmin** come nome del gruppo, oppure immettere un nome qualsiasi.

4. (Facoltativo) Immettere una descrizione per il gruppo.

5. Fare clic su Salva.

   **Nota:** non aggiungere l'appartenenza a un gruppo di applicazioni.

6. Fare clic su Chiudi.

## Concessione delle autorizzazioni al gruppo di amministratori della configurazione di ambiente

È possibile concedere autorizzazioni al gruppo personalizzato di amministratori della configurazione di ambiente aggiungendo il gruppo alle norme selezionate e selezionando le azioni richieste.

**Attenersi alla procedura seguente:**

1. Accedere all'applicazione CA Process Automation in CA EEM.
2. Fare clic sulla scheda di gestione delle norme di accesso.
3. Concedere al gruppo ConfigAdmin la possibilità di accedere a CA Process Automation e di visualizzare la pagina iniziale.
   a. Fare clic sul collegamento Utente del prodotto in Criteri di accesso.
   b. Fare clic sulla norma Accesso utente PAM40.
   c. Selezionare Application Group for Type (Gruppo applicazione per tipo) in Inserisci/Cerca identità, fare clic su Cerca identità, quindi su Cerca.
   d. Selezionare il gruppo personalizzato, ConfigAdmin, quindi fare clic sulla freccia giù.
   e. Selezionare Console_Login per la nuova identità.
   f. Fare clic su Salva.
4. Concedere al gruppo ConfigAdmins le autorizzazioni per bloccare un ambiente ed eseguire qualsiasi azione per la quale l'ambiente deve essere bloccato.
   a. Fare clic sul collegamento Ambiente nelle norme di accesso.
   b. Fare clic sul collegamento della norma ambiente PAM40 nella tabella delle norme.
   c. Aggiungere le identità. Cercare i gruppi. Selezionare Application Group for Type (Gruppo applicazione per tipo), fare clic su Cerca identità, quindi su Cerca.
   d. Selezionare ConfigAdmin e fare clic sulla freccia giù.
   e. Selezionare l'autorizzazione Environment_Configuration_Admin (amministratore configurazione).
   f. Fare clic su Salva. Fare clic su Chiudi.
5. Concedere al gruppo ConfigAdmin le autorizzazioni per accedere alla scheda Configurazione e installare gli orchestrator e gli agenti.
   a. Fare clic su Browser di configurazione.
   b. Fare clic su Norma di configurazione PAM40.
   c. Cercare ConfigAdmin e aggiungere il gruppo a Identità selezionate.
   d. Selezionare Client_Configuration_User (visualizzazione browser di configurazione) e Configuration_Installations.

6. Fare clic su Chiudi.

## Creazione di account utente per gli amministratori della configurazione di ambiente

È possibile creare account utente per le persone che eseguono il ruolo di amministratore della configurazione di ambiente.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestisci identità.
3. Fare clic su Nuovo utente.
4. Immettere l'ID utente in Nome.
5. Fare clic su Aggiungi informazioni su utente applicazione.
6. Selezionare il gruppo ConfigAdmin e fare clic sulla freccia destra.
7. Immettere i dettagli necessari di utente globale.
8. Immettere due volte una password temporanea nella sezione di autenticazione.
9. Fare clic su Salva.
10. Ripetere questa procedura per ciascun utente con il ruolo Amministratore della configurazione di ambiente.

## Creazione del gruppo ContentAdmin personalizzato

È possibile creare un gruppo personalizzato in CA EEM chiamato ContentAdmin per gli utenti presenti nel ruolo Amministratore del contenuto di ambiente. È possibile basare questo gruppo sul gruppo di progettazione predefinito per ottenere automaticamente le autorizzazioni assegnate al gruppo di progettazione.

**Attenersi alla procedura seguente:**

1. Accedere all'applicazione CA Process Automation in CA EEM.
2. Fare clic sulla scheda Gestisci identità.
3. Fare clic su Gruppi.
4. Fare clic su Nuovo gruppo applicazione.
5. Immettere ContentAdmin come nome del gruppo ed eventualmente una descrizione
6. Selezionare Designers (Responsabili di progettazione) in Gruppi utenti disponibili e fare clic sulla freccia destra per spostare i responsabili di progettazione nei gruppi utenti selezionati.
7. Fare clic su Salva.
8. Fare clic su Chiudi.

## Concessione delle autorizzazioni al gruppo ContentAdmin personalizzato

È possibile concedere le autorizzazioni al gruppo Amministratore del contenuto di ambiente personalizzato aggiungendo questo gruppo alle norme predefinite e selezionando le autorizzazioni richieste. Molte delle autorizzazioni sono già concesse a ContentAdmin perché il gruppo si basa sul gruppo di responsabili di progettazione predefinito. Si aggiungono i diritti di amministratore alle cartelle, agli oggetti di automazione e agli editor nella scheda Libreria.

**Attenersi alla procedura seguente:**

1. Accedere all'applicazione CA Process Automation in CA EEM.
2. Fare clic sulla scheda di gestione delle norme di accesso.
3. Fare clic sul collegamento Ambiente nelle norme di accesso.
4. Fare clic sul collegamento della norma ambiente PAM40 nella tabella delle norme.
5. Aggiungere le identità. Cercare i gruppi. Selezionare Application Group for Type (Gruppo applicazione per tipo), fare clic su Cerca identità, quindi su Cerca.
6. Selezionare ContentAdmin e fare clic sulla freccia giù.
7. Selezionare le autorizzazioni Environment_Library_Admin (amministratore del contenuto).
8. Fare clic su Salva.
9. Fare clic su Chiudi.

## Creazione di account utente per gli amministratori del contenuto di ambiente

È possibile creare account utente per le persone che eseguono il ruolo di amministratore del contenuto di ambiente.

**Attenersi alla procedura seguente:**

1. Cercare CA EEM ed eseguire l'accesso. (a pagina 45)
2. Fare clic sulla scheda Gestisci identità.
3. Fare clic su Nuovo utente.
4. Immettere l'ID utente in Nome.
5. Fare clic su Aggiungi informazioni su utente applicazione.
6. Selezionare il gruppo ContentAdmin e fare clic sulla freccia destra.
7. Immettere i dettagli necessari di utente globale.
8. Immettere due volte una password temporanea nella sezione di autenticazione.
9. Fare clic su Salva.
10. Ripetere questa procedura per ciascun utente con il ruolo Amministratore del contenuto di ambiente.

# Protezione touchpoint con CA EEM

Lo scopo di Protezione touchpoint è limitare l'accesso a host aziendali strategici o host con informazioni estremamente sensibili a un gruppo di utenti con privilegi elevati.

Questa sezione si applica solo se è abilitata Protezione touchpoint per touchpoint in uno o più ambienti.

- Per determinare se Protezione touchpoint è abilitata per touchpoint mappati su host candidati, rivedere la configurazione Protezione touchpoint nelle proprietà del touchpoint. Se è contrassegnato come Eredita dall'ambiente, si consiglia di modificare la configurazione in Abilitato.
- Per determinare se un touchpoint specifico di cui viene eseguito il mapping su un host che ha bisogno di protezione è protetto, rivedere i filtri nelle norme Protezione touchpoint.

**Ulteriori informazioni:**

Configurazione delle proprietà di dominio (a pagina 147)
Configurazione delle proprietà dell'ambiente (a pagina 159)
Configurazione delle proprietà per il touchpoint di progettazione (a pagina 226)
Configurazione delle proprietà Touchpoint dell'orchestrator (a pagina 176)
Introduzione alla configurazione di Protezione touchpoint (a pagina 150)

## Concessione agli utenti dell'accesso a CA EEM per definire le norme di protezione touchpoint

Per impostazione predefinita, l'utente EiamAdmin è l'unico utente in grado di accedere a CA EEM. Se si adotta un approccio di protezione touchpoint basato sulle norme, è possibile autorizzare determinati utenti a creare norme Protezione touchpoint in CA EEM. Autorizzare i responsabili di progettazione dei contenuti che progettano i processi con operatori eseguiti su touchpoint mappati su host di grande importanza per l'azienda. È possibile proteggere tali touchpoint con le norme Protezione touchpoint che specificano gli utenti autorizzati all'esecuzione di questi operatori.

**Per concedere ai responsabili specificati di progettazione norme l'accesso a CA EEM e l'autorizzazione a creare norme con la classe di risorsa Protezione touchpoint**

1. Accedere all'applicazione CA Process Automation in CA EEM.
2. Fare clic sulla scheda di gestione delle norme di accesso.
3. Fare clic su Nuova criterio di spazio.

4. Completare la sezione Generale come segue:

**Nome**

Specifica il nome della norma di ambito. Ad esempio, Utenti autori di norme per protezione touchpoint.

**Descrizione**

(Facoltativo) Offre una breve descrizione. Ad esempio, consente agli utenti specificati di creare norme personalizzate solo con la classe di risorsa Protezione touchpoint.

**Calendario e Nome classe risorsa**

Ignorare l'opzione Calendario e accettare la voce predefinita SafeObject per il nome di classe di risorsa.

**Tipo**

Specificare Elenco controllo accesso.

**Nota:** viene visualizzato un messaggio per indicare che la modifica del tipo di norma reimposta alcuni filtri. Fare clic su OK.

5. In Identità aggiungere i nomi di tutti gli utenti che progettano processi a cui si applica la norma Protezione touchpoint. Agli utenti aggiunti a questa norma vengono concessi diritti di accesso a CA EEM e la possibilità di creare norme Protezione touchpoint. Una norma Protezione touchpoint specifica gli utenti da autorizzare per l'esecuzione di operatori di una data categoria operatore su un touchpoint specifico.

   **Nota:** se si desidera verificare questa norma, creare un utente con il gruppo utenti predefinito e aggiungervi il nome utente. Dopo avere salvato questa norma, accedere a CA EEM con il nome utente di test. Nota: l'unica azione consentita in CA EEM è la creazione di una norma con la classe risorsa di Touchpoint.

   a. Accettare Utente come Tipo o selezionare un altro valore.

   b. Fare clic sul collegamento Cerca identità.

   c. Immettere i criteri di ricerca che includono l'utente pianificato o il gruppo e fare clic su Cerca.\

   d. Selezionare un utente o gruppo dall'elenco visualizzato delle identità disponibili e fare clic sulla freccia destra.

      L'utente o il gruppo selezionato viene visualizzato nell'elenco Identità selezionate.

   e. Ripetere questa procedura per ciascun utente che si desidera autorizzare per la creazione di norme Protezione touchpoint.

6. Configurare l'elenco di controllo di accesso come segue:

   a. Selezionare tutte le risorse seguenti dall'elenco a discesa e fare clic su Aggiungi per aggiungerle all'elenco.

      - ApplicationInstance
      - Norma
      - Utente
      - GlobalUser
      - UserGroup
      - GlobalUserGroup

   b. Fare clic su leggi per tutte le risorse. Fare clic su scrivi per Norma

   c. Fare clic su Filtri.

   d. Per Norma, selezionare l'attributo denominato dal primo elenco a discesa. Nel campo in corrispondenza dell'attributo denominato, immettere ResourceClassName. Nel campo di valore dopo EQUAL, immettere TouchPointSecurity. Non immettere uno spazio tra TouchPoint e Security.

   e. Lasciare invariato il resto dei campi nella pagina dei filtri.

7. Fare clic su Salva.

8. Verificare che Configurazione elenco controllo accesso corrisponda esattamente all'esempio seguente. Il sistema aggiunge uno spazio tra TouchPoint e Security.

9. Verificare che la norma sia analoga all'esempio seguente. Nell'esempio, le colonne mancanti indicano che ResourceClassName è SafeObject, il valore Opzioni è Concessione esplicita e Identità è il proprio elenco di utenti. Questi sono gli utenti che progettano i processi per Protezione touchpoint e creano una norma associata.

Criteri di ambito

| Nome/Descrizione | Azioni | Risorse | Filtri | | | | | |
|---|---|---|---|---|---|---|---|---|
| Users Defining Touchpoint Security Policies<br>Enables specified users to create custom policies only with the TouchPoint Security resource class. | read<br>write | ApplicationInstance<br>Policy<br>GlobalUser<br>User<br>UserGroup<br>GlobalUserGroup | DOVE | ( | req:resource | == val:ApplicationInstance | | ApplicationInstanc |
| | | | E | | req:action | {} val:read | ) | ApplicationInstanc |
| | | | O | ( | req:resource | == val:Policy | | Policy |
| | | | E | | req:action | {} val:read,write | | Policy |
| | | | E | | name:ResourceClassName | == val:TouchPointSecurity | ) | Policy |
| | | | O | ( | req:resource | == val:User | | User |
| | | | E | | req:action | {} val:read | ) | User |
| | | | O | ( | req:resource | == val:GlobalUser | | GlobalUser |
| | | | E | | req:action | {} val:read | ) | GlobalUser |
| | | | O | ( | req:resource | == val:UserGroup | | UserGroup |
| | | | E | | req:action | {} val:read | ) | UserGroup |
| | | | O | ( | req:resource | == val:GlobalUserGroup | | GlobalUserGroup |
| | | | E | | req:action | {} val:read | ) | GlobalUserGroup |

## Informazioni sulla protezione del touchpoint

La protezione del touchpoint consente di proteggere i touchpoint associati a host aziendali strategici e gli host contenenti dati sensibili dagli accessi non autorizzati. È possibile creare norme di touchpoint che specificano gli utenti selezionati o un gruppo con privilegi elevati quali uniche identità in grado di eseguire un operatore su quella destinazione. Le norme specificano le identità autorizzate all'esecuzione di determinati operatori su touchpoint specifici. Gli operatori che eseguono programmi e script sono contenuti in categorie operatori specifiche.

In breve, le norme Protezione touchpoint di CA EEM autorizzano identità specifiche a eseguire script in operatori di categorie operatori specifiche su touchpoint specifici in un ambiente specifico.

Di seguito si riporta un breve esempio di una norma di protezione touchpoint semplice.

| Identità | Azioni | Risorse | Filtri | | | |
|---|---|---|---|---|---|---|
| ug:High-PrivilegedUsers | [Tutte le azioni] | ✔ Confronto regex<br>Network Utilities Module<br>Process Module<br>File Module | DOVE | ( | name:ENVIRONMENT | == val:Production |
| | | | E | ( | name:TOUCHPOINT | == val:SensitiveHostTP1 |
| | | | O | | name:TOUCHPOINT | == val:SensitiveHostTP2 |
| | | | O | | name:TOUCHPOINT | == val:SensitiveHostTP3 )) |

L'esempio utilizza un estratto di norma. La norma consente solo agli utenti nel gruppo High-PrivilegedUsers di eseguire qualsiasi operatore appartenente alle categorie specificate su touchpoint nell'ambiente di produzione. I touchpoint di esempio sono denominati SensitiveHostTP1, 2 e 3. Gli ID di Access Control specificati includono il modulo Utilità di rete e il modulo Processo (per Esecuzione comando). Il modulo File* include sia il modulo per Gestione file sia il modulo Trasferimento file.

Nota: consultare la sezione Identificazione degli ID controllo accesso da aggiungere come risorse (a pagina 129).

Un processo contenente una destinazione di operatore protetta da una norma Protezione touchpoint può terminare correttamente solo se eseguito da utente autorizzato. L'utente che esegue il processo viene indicato come Identità nella norma. La norma identifica gli utenti in base al nome o all'appartenenza a un gruppo, gli operatori in base agli ID di Access Control associati alle categorie di origine e i touchpoint in base a nome, ambiente o entrambi.

Le norme Protezione touchpoint proteggono l'accesso ai singoli host di destinazione controllando quali utenti eseguono gli operatori su un touchpoint o un gruppo host specifico. Un'istanza di processo viene eseguita per conto di un utente. Quando il processo esegue un operatore su un touchpoint o un gruppo host specificato in una norma Protezione touchpoint di CA EEM, CA EEM tenta di autorizzare tale utente. CA EEM verifica che l'utente sia stato specificato come Identità in una norma Protezione touchpoint per il touchpoint. Se l'istanza di processo viene eseguita per conto di un utente non autorizzato, si verificherà un errore dell'operatore.

Specificare gli host contenenti informazioni sensibili come touchpoint, touchpoint proxy o gruppi host.

È possibile limitare l'accesso a host specifici agli utenti con privilegi elevati. È possibile concedere l'accesso a un utente o a un gruppo specifici a cui è stato concesso il seguente accesso:

- Azione Console_Login (Utente) concessa nella norma Accesso utente PAM40.
- Azione Environment_Library_User (User) concessa nella norma Ambiente PAM40.

**Ulteriori informazioni:**

Creazione di una policy Protezione touchpoint (a pagina 130)
Concessione agli utenti dell'accesso a CA EEM per definire le norme di protezione touchpoint (a pagina 121)

## Scenari di utilizzo: Casi in cui la protezione touchpoint è necessaria

La protezione touchpoint è necessaria nei casi seguenti:

- Un host dell'ambiente in uso, ad esempio una destinazione di operatore, contiene informazioni sensibili, quali codice fiscale, numeri di carta di credito o dati sanitari. Si desidera limitare l'accesso a questo processo sensibile a un solo utente o a un piccolo gruppo con privilegi elevati.

  È possibile utilizzare uno dei seguenti host come destinazione:

  - L'host con un agente associato a un touchpoint.
  - L'host con un agente associato a un touchpoint proxy e connessione SSH a un host remoto.
  - L'host con un agente associato a un gruppo host di riferimento e con una connessione a host remoti.

- Quando è in corso l'esecuzione di un agente su un host come utente principale (UNIX), amministratore (Windows) o utente con diritti specifici e si desidera eseguire tutti gli script e i programmi su tale agente con la stessa identità dell'agente. Ovvero, non si desidera utilizzare un altro utente che richiede credenziali. Per evitare rischi di protezione, è possibile impedire agli utenti con privilegi limitati di eseguire gli script con la stessa identità dell'agente, ad esempio l'utente principale.

- Quando si utilizzano gruppi host che definiscono le credenziali predefinite del sistema operativo per l'esecuzione di operatori Esecuzione comando su subnet intere. Si desidera eseguire tutti gli script e i programmi su tale gruppo host utilizzando le credenziali del sistema operativo. Per impedire rischi di protezione, non consentire agli utenti con privilegi ridotti di creare ed eseguire script utilizzando le credenziali di sistema operativo.

- Gli utenti che eseguono un processo possono selezionare le destinazioni di operatore in fase di runtime per gli operatori con una variabile nel campo di destinazione. Generalmente, una destinazione di operatore corrisponde a un touchpoint, tuttavia può corrispondere anche a un touchpoint proxy, un nome di dominio completo oppure a un indirizzo IP di riferimento di un gruppo host. Questa progettazione flessibile consente a qualsiasi utente autorizzato di eseguire il processo per selezionare una destinazione in fase di runtime.

  Si riscontra un problema di protezione quando è necessario porre dei limiti all'accesso di un touchpoint disponibile. Considerare il caso in cui un operatore può essere eseguito correttamente su due touchpoint diversi, ognuno dei quali rappresenta un'applicazione Service Desk. Un touchpoint rappresenta un'applicazione Service Desk progettata per l'accesso generale, mentre l'altro è progettato solo per gli amministratori. La protezione touchpoint permette solo agli amministratori di eseguire questo operatore di esempio sul touchpoint progettato per loro. Le policy Protezione touchpoint in CA EEM limitano l'accesso.

La protezione del touchpoint è anche utile per i responsabili di progettazione dei processi. Durante lo sviluppo dei processi, i responsabili di progettazione installano un agente sui propri host personali e creano i touchpoint per i propri agenti. In genere, i responsabili di progettazione non desiderano che altri utenti eseguano operatori sui propri host locali. La protezione del touchpoint è in grado di fornire questa protezione. Se la protezione del touchpoint è attiva, l'autorizzazione per eseguire ciascun operatore sulla destinazione selezionata viene verificata in fase di runtime. L'applicazione della policy consente agli utenti che eseguono un processo di eseguire gli operatori unicamente sui touchpoint per cui dispongono dell'autorizzazione.

## Limitazione dell'accesso agli host con informazioni sensibili

La protezione del touchpoint risponde alla necessità di limitare l'accesso agli host aziendali strategici e agli host di archiviazione delle informazioni riservate. L'illustrazione seguente descrive la procedura che consente di realizzare questo obiettivo di protezione.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Creare un gruppo di utenti con privilegi elevati.

   Consultare la sezione Creazione del gruppo ContentAdmin personalizzato (a pagina 118).
3. Identificare i touchpoint associati a host sensibili.

   Consultare la sezione Visualizzazione dei touchpoint e dei gruppi host per un agente selezionato (a pagina 212).
4. Identificare le categorie con operatori che espongono i dati.
5. Identificare gli ID controllo accesso associati alle categorie.
   - Consultare la sezione Esempio: Protezione di touchpoint critici (a pagina 132) per gli ID di Access Control da considerare.
   - Le descrizioni di ciascuna categoria sono disponibili nella sezione Categorie operatore e posizione di esecuzione degli operatori (a pagina 321).
   - Per le descrizioni degli operatori, consultare la *Guida di riferimento per la progettazione dei contenuti*.
6. Creare una policy Protezione touchpoint con questo gruppo, categorie operatori e touchpoint.

   Consultare la sezione Creazione di una policy Protezione touchpoint (a pagina 130).
7. Abilitare Protezione touchpoint sui touchpoint selezionati.
   - Consultare la sezione Configurazione delle proprietà dei touchpoint (a pagina 226).
   - Consultare la sezione Configurazione delle proprietà dei touchpoint proxy (a pagina 249).
   - Consultare la sezione Configurazione delle proprietà del gruppo host (a pagina 257).

**Ulteriori informazioni:**

Introduzione alla configurazione di Protezione touchpoint (a pagina 150)

## Identificazione degli ID controllo accesso da aggiungere come risorse

Quando si crea una policy Protezione touchpoint, gli operatori che agiscono sui touchpoint da proteggere non vengono identificati direttamente.. Piuttosto, identificare le categorie a cui appartengono tali operatori. Identificareo le categorie non in base al nome, bensì all'ID controllo accesso.

Non tutte le categorie contengono operatori che potrebbero compromettere la protezione di un host con informazioni sensibili. Valutare l'impatto degli operatori prima di aggiungere le risorse.

È possibile identificare l'ID controllo accesso da aggiungere come risorsa a una policy Protezione touchpoint.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA Process Automation (a pagina 18).
2. Fare clic sulla scheda Configurazione.
3. Selezionare un agente dal nodo Agenti, quindi selezionare la scheda Moduli.
4. Annotare i nomi come sono visualizzati nella colonna ID controllo accesso.

| Nome | Attiva/Disattiva | ID controllo accesso |
|---|---|---|
| Catalyst | | Catalyst Module |
| Controllo processo | | Workflow Module |
| Data-Ora | | Date-Time Module |
| Database | Eredita dall'ambiente | JDBC Module |
| Esecuzione comando | Eredita dall'ambiente | Process Module |
| Gestione file | Eredita dall'ambiente | File Module |
| Gestione Java | Eredita dall'ambiente | JMX Module |
| Posta elettronica | Eredita dall'ambiente | Mail Module |
| Servizi directory | Eredita dall'ambiente | LDAP Module |
| Servizi Web | Eredita dall'ambiente | SOAP Module |
| Trasferimento file | Eredita dall'ambiente | File Transfer Module |
| Utilità | Eredita dall'ambiente | Utilities Module |
| Utilità di rete | Eredita dall'ambiente | Network Utilities Module |

**Importante.** La colonna ID controllo accesso elenca i nomi di modulo. Fare riferimento a questo elenco quando si immettono i nomi di modulo selezionati nel campo Risorse in una policy Protezione touchpoint.

## Creazione di una policy Protezione touchpoint

L'esecuzione di un processo comporta l'esecuzione di operatori specifici su destinazioni precise secondo una determinata sequenza. Una policy personalizzata Protezione touchpoint concede l'autorizzazione a utenti o gruppi specificati per l'esecuzione di determinati operatori su destinazioni precise. Gli amministratori di CA EEM possono creare una policy di protezione touchpoint.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda Gestione criteri di accesso.
3. Fare clic sul pulsante Nuovo criterio di accesso per Protezione touchpoint in Criteri di accesso.
4. Nel modulo del nuovo criterio di accesso per la classe di risorsa Protezione touchpoint, immettere un nome per la policy personalizzata Protezione touchpoint.

   La sezione Inserisci/Cerca identità consente di specificare l'utente o il gruppo di destinazione.
5. Selezionare il tipo di destinazione a cui concedere l'accesso:
   - Selezionare Utente se la destinazione è un utente globale.
   - Selezionare Gruppo globale se la destinazione è un gruppo da un archivio utenti di riferimento.
   - Selezionare Gruppo applicazione se la destinazione è un gruppo personalizzato oppure un gruppo predefinito.
6. Fare clic su Cerca identità.
7. Selezionare le identità a cui si applica questa policy, quindi fare clic sulla freccia giù.

   Nell'elenco Identità selezionate è visualizzata la selezione dell'utente.
8. Selezionare l'azione Esegui.

9. Nel campo Aggiungi risorsa, immettere l'ID controllo accesso per la categoria dell'operatore di origine che include gli operatori a cui si applica questa policy. Ad esempio:

   - Immettere il **modulo di processo** per la categoria di operatore Esecuzione comando.
   - Immettere il **modulo di file** per la categoria di operatore Gestione file.
   - Immettere il **modulo di trasferimento file** per la categoria di operatore Trasferimento file.
   - Immettere il **modulo dell'utilità di rete** per la categoria di operatore Utilità di rete.

   È possibile immettere espressioni regolari per includere le categorie operatore appropriate, quindi selezionare Tratta i nomi risorse come espressioni regolari. Ad esempio, la voce *file includerebbe gli operatori delle categorie Gestione file e Trasferimento file.

10. Fare clic su Aggiungi.
11. Aggiungere un filtro che indica l'ambiente con le destinazioni della policy:
    - Impostare l'attributo denominato su Ambiente.
    - Impostare l'operatore STRINGA su UGUALE.
    - Impostare il valore su *environment_name*.
12. Aggiungere altri filtri che specificano le destinazioni in base al nome di touchpoint:
    - Impostare l'attributo denominato su Touchpoint.
    - Impostare l'operatore STRINGA su UGUALE.
    - Impostare il valore su *touchpoint_name*.
13. Fare clic su Salva.

    Se le policy Protezione touchpoint sono configurate per l'applicazione, queste vengono valutate e applicate.

## Esempio: touchpoint critici protetti

Protezione touchpoint garantisce che la possibilità di eseguire gli operatori su host aziendali strategici sia limitata a un piccolo gruppo di utenti con privilegi elevati. Il modo più facile per proteggere host sensibili è creare una policy Protezione touchpoint ed elencare ognuno dei touchpoint associati in un filtro. Quindi, abilitare Protezione touchpoint sull'impostazione di proprietà per ciascun touchpoint.

### Esempio: configurazione di Protezione touchpoint per un touchpoint critico

L'esempio seguente mostra le proprietà di un touchpoint selezionato. Quando Protezione touchpoint è impostata su Abilitato, il processo valuta ogni tentativo di eseguire un operatore su questo touchpoint rispetto alle policy Protezione touchpoint.

### Esempio: policy Protezione touchpoint per touchpoint critici

Per garantire che solo gli utenti con privilegi elevati eseguano gli operatori su host sensibili nel proprio ambiente di produzione, creare una policy Protezione touchpoint. Nella policy Protezione touchpoint, aggiungere l'ID di controllo dell'accesso associato a ciascuna categoria contenente operatori che potrebbero rappresentare un rischio. Aggiungere un filtro per l'ambiente in uso. Aggiungere un filtro per ciascun touchpoint che fa riferimento agli host sensibili.

Considerare la policy Protezione touchpoint globale di esempio. La policy di esempio consente al gruppo di utenti con privilegi elevati di eseguire script o programmi utilizzando operatori in cinque categorie su touchpoint con rischio elevato. Gli ID di Access Control rappresentano le cinque categorie. Questa policy si applica ai touchpoint specificati solo nell'ambiente di produzione.

Criteri di accesso - "TouchPointSecurity"

| Nome/Descrizione | ResourceClassName | Opzioni |
|---|---|---|
| Global TouchPoint Security Policy<br>Authorizes High-Privileged group to execute risk posing Operators on Sensitive Hosts in Production. | TouchPointSecurity | Concessione esplicita |

| Identità | Azioni | Risorse | Filtri | | | |
|---|---|---|---|---|---|---|
| ug:High-PrivilegedUsers | Execute | Process Module<br>File Module<br>File Transfer Module<br>JMX Module<br>Network Utilities Module | DOVE | name:ENVIRONMENT | == | val:Production |
| | | | E | name:TOUCHPOINT | == | val:TP-SensitiveHost1 |
| | | | O | name:TOUCHPOINT | == | val:TP-SensitiveHost2 |
| | | | O | name:TOUCHPOINT | == | val:TP-SensitiveHost3 |
| | | | O | name:TOUCHPOINT | == | val:TP-SensitiveHost4 |
| | | | O | name:TOUCHPOINT | == | val:TP-SensitiveHostn |

## Esempio: protezione del touchpoint per l'host personale

Supporre di installare un agente sul proprio host, ma non si desidera che altri utenti esterni eseguano operatori sull'host personale. Per utilizzare Protezione touchpoint in modo da proteggere un host considerato importante, valutare l'esecuzione di attività necessarie nella sequenza proposta.

1. Installare un agente sull'host.
2. Associare un touchpoint in un ambiente specificato con tale host.
3. Creare una norma Protezione touchpoint che indichi l'utente attuale come identità. Aggiungere l'ID di Access Control per ciascuna categoria con operatori che possono essere eseguiti su touchpoint associati ad agenti.
4. Configurare Protezione touchpoint come Abilitato nelle proprietà del touchpoint per tale host.

### Esempio: impostazione di Protezione touchpoint su Abilitato per il touchpoint del computer personale

Il parametro Protezione touchpoint per il touchpoint selezionato, MyPC-TP, è impostato su Abilitato.

### Esempio: Creazione di una norma Protezione touchpoint che consenta l'esecuzione degli operatori sul touchpoint del computer personale solo all'utente corrente

Nell'esempio seguente,l'host protetto appartiene a un utente denominato MyPCowner. MyPCowner è l'unica identità autorizzata all'esecuzione di operatori sul touchpoint, MyPC-TP. In questo caso, gli ID di controllo degli accessi vengono associati a tutte le categorie contenenti operatori che possono essere eseguiti su un host agente. I riferimenti comprendono le categorie di operatori che non apportano modifiche all'host. In questo esempio, l'utente non desidera che altri utenti esterni accedano all'host associato al touchpoint MyPC-TP. Solo MyPCowner può eseguire processi su MyPC-TP quando è abilitata Protezione touchpoint.

| Secure TP My PC | TouchPointSecurity | Concessione esplicita |
|---|---|---|

Il nome del touchpoint viene specificato come valore nel filtro.

| MyPCOwner | Execute | Process Module<br>JDBC Module<br>LDAP Module<br>Mail Module<br>File Module<br>File Transfer Module<br>JMX Module<br>Network Utilities Module<br>Utilities Module<br>SOAP Module | **DOVE** name:ENVIRONMENT == val:Test<br>**E** name:TOUCHPOINT == val:MyPC-TP |
|---|---|---|---|

# Autorizzazione di azioni di runtime con CA EEM

CA Process Automation consente il controllo dell'accesso dettagliato per operazioni e azioni utente su oggetti di automazione specifici, quali processi, set di dati, calendari e pianificazioni. Il controllo include i tipici diritti di lettura/scrittura e i diritti di avvio processo e monitoraggio delle istanze. I diritti di accesso vengono applicati a tutte le interfacce esterne, tra cui l'interfaccia utente di CA Process Automation e i servizi Web. Inoltre, CA Process Automation consente di proteggere le operazioni su host di destinazione in modo che solo gli utenti autorizzati possano eseguirli.

Per limitare gli utenti autorizzati a eseguire una qualsiasi delle seguenti azioni di runtime, creare una norma di CA EEM e specificare gli utenti o il gruppo da autorizzare.

- Eseguire script o i programmi in operatori derivati da categorie specificate che utilizzano come destinazione touchpoint specifici in un ambiente determinato.
- Controllare una pianificazione, nonché attivarla e disattivarla.
- Controllare o modificare un set di dati.
- Controllare un'istanza del processo, nonché sospenderla, riavviarla, riprenderla e interromperla.
- Controllare una risorsa, nonché bloccarla, sbloccarla, accettarla, restituirla o aggiungervi una variabile. Aggiungere o rimuovere un'unità di risorsa.
- Rimuovere dalla coda o avviare un modulo di richiesta di avvio.

Inoltre, è possibile creare una norma che concede diritti di lettura/scrittura per qualsiasi altro oggetto di automazione.

**Ulteriori informazioni:**

Autorizzazioni per gli oggetti di automazione (a pagina 106)
Dipendenze delle autorizzazioni (a pagina 109)
Filtri per autorizzazioni (a pagina 112)

# Modifica della proprietà per oggetti di automazione

L'utente che crea un oggetto di automazione o una cartella è, per impostazione predefinita, il titolare. Il titolare ha il controllo completo dell'oggetto di automazione o della cartella. Un titolare può cambiare la titolarità impostandola su un altro utente di CA Process Automation.

**Nota:** L'autorizzazione CA EEM Environment_Content_Administrator concede il controllo completo di tutti gli oggetti di automazione e delle cartelle. Tutti gli amministratori che appartengono al gruppo PAMAdmins dispongono di questa autorizzazione.

Se si abilita la protezione runtime, solo il titolare del processo (o un amministratore) può avviare tale processo.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Selezionare uno o più oggetti, incluse le cartelle.
3. Fare clic sul pulsante Imposta titolare nella barra degli strumenti.
4. Nell'elenco Utenti disponibili, scegliere l'account dell'utente che si desidera impostare come nuovo titolare. Utilizzare la ricerca per trovare account utenti corrispondenti.
5. Fare clic su Salva e chiudi.

# Capitolo 5: Amministrazione del dominio di CA Process Automation

In CA Process Automation, il dominio comprende l'intero sistema. L'amministrazione del dominio comprende tutte le attività che possono essere eseguite solo da un amministratore con diritti Amministratore di dominio. Le attività comprendono l'aggiunta di ambienti, la rimozione in blocco di agenti e touchpoint inutilizzati, nonché la configurazione di protezione, proprietà, categorie di operatori e trigger a livello di dominio. Questo capitolo è dedicato esclusivamente alle attività eseguite durante la configurazione iniziale di un sistema CA Process Automation appena installato. I capitoli successivi tratteranno invece le attività che vengono generalmente eseguite durante lo sviluppo dei contenuti.

Questa sezione contiene i seguenti argomenti:



## Blocco del dominio

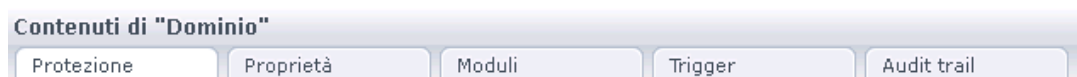
Il dominio può essere bloccato dagli amministratori. Un blocco evita aggiornamenti simultanei del dominio apportati da più utenti. Prima di apportare qualsiasi modifica alla configurazione a livello di dominio, bloccare il dominio.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Selezionare Dominio nel riquadro Browser di configurazione e fare clic su Blocca.

Dopo aver completato le modifiche alla configurazione, selezionare Dominio e fare clic su Sblocca.

## Configurazione dei contenuti del dominio

Selezionare Dominio nel Browser di configurazione, per visualizzare le schede seguenti nei contenuti di Dominio:

- Protezione

  Consultare la sezione Configurazione delle impostazioni di protezione di CA EEM per il dominio (a pagina 140).

- Proprietà

  Consultare la sezione Configurazione delle proprietà di dominio (a pagina 147).

- moduli

  Consultare la sezione Configurazione delle categorie operatore (a pagina 276). Dopo questo argomento segue la procedura di configurazione per ciascuna categoria operatore. Prima di ciascuna procedura di configurazione vengono descritte le singole categorie.

- trigger

  Consultare la sezione Modalità di configurazione e utilizzo di trigger (a pagina 324). A questo argomento seguono i dettagli di configurazione per ciascun tipo di trigger.

- Audit Trail

  Consultare la sezione Visualizzazione dell'itinerario di controllo per il dominio (a pagina 345).

**Ulteriori informazioni:**

Gestione del dominio (a pagina 395)

## Informazioni sull'ereditarietà di configurazione

La configurazione a livello di dominio include i seguenti tipi di impostazioni:

- Protezione
- Proprietà
- Categorie di operatori
- trigger

Gli oggetti figlio del dominio includono l'ambiente predefinito, gli ambienti definiti dall'utente, gli agenti e l'orchestrator di dominio. Gli oggetti figlio di un determinato ambiente includono orchestrator definiti dall'utente, touchpoint - inclusi touchpoint proxy - e gruppi host.

Alcune impostazioni configurate a livello di dominio sono, per impostazione predefinita, ereditate da tutti o da alcuni oggetti figlio all'interno del dominio. Ad esempio, tutti gli ambienti possono ereditare le impostazioni della categoria operatore dal dominio. Gli orchestrator possono ereditare impostazioni della categoria operatore dal loro ambiente.

Poiché gli agenti possono operare tra ambienti, l'ereditarietà può derivare direttamente dal dominio o dall'ambiente, in base alla configurazione dell'ambiente. Le impostazioni della categoria operatore sono sostituibili a livello di agente. Gli agenti ereditano l'impostazione di proprietà della frequenza heartbeat direttamente dal dominio.

In genere, le configurazioni vengono ereditate per impostazione predefinita. I trigger costituiscono un'eccezione. Le configurazioni dei trigger sono disabilitate per impostazione predefinita ai livelli inferiori, ma possono essere ereditate dopo la loro abilitazione.

## Configurazione delle impostazioni di protezione di CA EEM per il dominio

La maggior parte delle impostazioni di protezione di CA EEM viene stabilita durante l'installazione dell'orchestrator di dominio. Una istanza di CA EEM gestisce la protezione del dominio di CA Process Automation. Pertanto, le stesse impostazioni sono valide per tutti gli ambienti nel dominio e per tutti gli orchestrator all'interno di tutti gli ambienti. È possibile modificare le impostazioni di sola lettura reinstallando l'orchestrator di dominio.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.

   Viene visualizzata la scheda Protezione.

2. Esaminare le impostazioni che sono state create durante l'installazione. Ad esempio, Nome applicazione EEM è il valore che va immesso per Applicazione nei casi seguenti:

   - Quando si accede a CA EEM per creare gli account utente.
   - Quando si assegnano gruppi predefiniti a utenti nuovi o di riferimento.

3. Esaminare il valore Intervallo di aggiornamento della cache CA EEM.

   Questo valore esprime l'intervallo (in secondi) tra gli aggiornamenti della cache di CA EEM. La cache di CA EEM contiene le impostazioni correnti per account utente di CA Process Automation, gruppi e policy. Quando CA EEM aggiorna la cache, invia a CA Process Automation i contenuti della cache aggiornata. Il valore predefinito, che ottimizza le prestazioni di sistema, è 1800 secondi (30 minuti).

   - Il valore predefinito è adeguato una volta configurati tutti gli utenti in CA EEM.
   - Per velocizzare questa attività, ridurre l'intervallo di aggiornamento al minimo (60 secondi) in fase di test e perfezionamento delle policy personalizzate. Valutare la riduzione dell'intervallo a livello di ambiente per l'ambiente sottoposto a test.

4. Esaminare il valore Dominio Active Directory predefinito, se impostato.

   Questo valore è impostato solo se CA EEM è configurato per l'utilizzo di un archivio utenti esterno e l'opzione Più domini Microsoft Active Directory è selezionata. Gli utenti di CA Process Automation di riferimento nel dominio qui specificato possono accedere con un nome utente non completo. Gli utenti di CA Process Automation di riferimento in altri domini Active Directory selezionati vengono autenticati con i rispettivi nomi principali (ovvero, *domain_name**user_name*). La stessa differenza nelle convenzioni di denominazione si estende al modo in cui si fa riferimento alle identità dell'utente nel riquadro principale della scheda Libreria.

5. Per reimpostare uno dei valori modificabili:

   a. Selezionare il nodo Dominio e fare clic su Blocca.

   b. Selezionare un nuovo valore.

   c. Fare clic su Salva.

   d. Selezionare il nodo Dominio e fare clic su Sblocca.

   Se è stato ridotto l'intervallo di aggiornamento della cache di CA EEM, considerare l'eliminazione della cache per le autorizzazioni di CA Process Automation. Consultare la sezione Controllo delle cache per gli aggiornamenti di CA EEM (a pagina 78).

**Ulteriori informazioni:**

Controllo delle cache per gli aggiornamenti di CA EEM (a pagina 78)
Gestione certificati (a pagina 398)
Avvio dell'orchestrator (a pagina 197)

## Modifica dell'impostazione di protezione in modalità FIPS di CA EEM

Durante l'installazione, la proprietà di modalità FIPS di CA EEM viene impostata su attiva o disattivata. Questa impostazione determina gli algoritmi utilizzati per crittografare i dati trasferiti tra CA EEM e CA Process Automation. Quando la modalità FIPS è attiva, gli algoritmi sono compatibili con FIPS 140-2. Quando CA Process Automation è installato con un'applicazione CA EEM configurata con la modalità FIPS attiva, l'impostazione di certificato di conformità FIPS viene visualizzata come selezionata.

È possibile modificare l'impostazione di protezione del certificato di conformità FIPS ai livelli seguenti:

- Dominio
- Ambienti
- Orchestrator

Indipendentemente dal livello in cui viene modificata l'impostazione del certificato di conformità FIPS, tale modifica ha un impatto sul dominio intero. Il dominio dispone di un'applicazione CA EEM. L'impostazione del certificato di conformità FIPS influisce anche sull'impostazione di modalità FIPS di CA EEM e sull'impostazione del file iGateway.

**Importante.** Consultare l'amministratore di dominio prima di modificare qualsiasi impostazione di protezione in CA EEM. Le impostazioni di protezione hanno un impatto notevole.

**Attenersi alla procedura seguente:**

1. Ottenere la password di certificato EEM dal programma di installazione.
2. Arrestare CA Process Automation su tutti gli orchestrator eccetto che sull'orchestrator di dominio, se applicabile.
3. Accedere al server in cui è installato l'orchestrator di dominio di CA Process Automation e procedere come segue:
    a. Arrestare CA Process Automation.
    b. Arrestare il servizio dell'orchestrator. Ad esempio, dal menu Start di Windows selezionare CA, CA Process Automation 4.0, Arresta servizio dell'orchestrator.
4. Accedere al server in cui è installato CA EEM e procedere come segue:
    a. Arrestare CA EEM.
    b. Interrompere il servizio CA iTechnology iGateway.

5. Accedere alla cartella ...\CA\SharedComponents\iTechnology.
6. Modificare l'impostazione di modalità FIPS nel file igateway.conf.
   a. Aprire igateway.conf per modificarlo. Ad esempio, fare clic con il pulsante destro del mouse su igateway.conf e selezionare la modifica con Notepad++.
   b. Individuare la riga con l'impostazione FIPSMode. Ad esempio:

      ```
      Riga 4: <FIPSMode>off</FIPSMode>
      ```

   c. Modificare il valore da disattivato ad attivo o viceversa.
   d. Salvare il file e chiuderlo.
7. Eseguire iGateway Certificate Utility (igwCertUtil) per convertire i tipi di certificato di CA EEM come segue:
   - In caso di attivazione della modalità FIPS di CA EEM (tramite selezione di una casella di controllo deselezionata), procedere come segue:
     - Creare un tipo di certificato pem, PAM.cer e PAM.key.
     - Sostituire il certificato PAM.p12 con il tipo di certificato pem.
   - In caso di disattivazione della modalità FIPS di CA EEM (tramite deselezione di una casella di controllo selezionata), sostituire PAM.cer e PAM.key con PAM.p12 e una password.

     **Nota:** per informazioni, consultare la sezione Esempi d'uso di iGateway Certificate Utility (a pagina 145).
8. Riavviare il servizio iGateway.
9. Riavviare CA EEM con l'impostazione di modalità FIPS appropriata.
10. Riavviare il servizio dell'orchestrator sul server con l'orchestrator di dominio.
    - Interrompere l'orchestrator (a pagina 196).
    - Avviare l'orchestrator (a pagina 197).

11. Accedere a CA Process Automation e visualizzare l'impostazione di protezione del certificato di conformità FIPS e le impostazioni correlate come segue:
    a. Accedere a CA Process Automation e fare clic sulla scheda Configurazione.
    b. Accedere al livello in cui si desidera implementare la modifica e bloccarlo (Dominio, Ambiente o Orchestrator).
    c. Visualizzare la casella di controllo Certificato di conformità FIPS.
    d. Se la modifica ha attivato la modalità FIPS per CA EEM, procedere come segue:
        - Verificare che l'opzione Certificato di conformità FIPS sia selezionata. In caso contrario, selezionarla.
        - Immettere la chiave generata nel campo Chiave del certificato CA EEM.
    e. Se la modifica ha disattivato la modalità FIPS per CA EEM, procedere come segue:
        - Verificare che l'opzione Certificato di conformità FIPS sia deselezionata. In caso contrario, deselezionarla.
        - Immettere la password generata nel campo Password di certificato CA EEM.
    f. Fare clic su Salva.
    g. Sbloccare il livello di dominio e ambiente dal riquadro Browser o di orchestrator dal riquadro Orchestrator.
12. Riavviare CA Process Automation sui server con orchestrator che non sono orchestrator di dominio.

## Esempi d'uso di iGateway Certificate Utility

È possibile modificare l'impostazione protezione della modalità FIPS di CA EEM dall'impostazione configurata in fase di installazione. Parte di questo processo di modifica implica l'utilizzo di iGateway Certificate Utility (igwCertUtil). È possibile trovare questo file in ...\CA\SharedComponents\iTechnology\igwCertUtil.exe.

**Nota:** per informazioni, consultare la sezione Modifica dell'impostazione di protezione per la modalità FIPS di CA EEM (a pagina 142).

iGateway Certificate Utility offre le funzionalità descritte negli esempi seguenti:

### Esempio: creare un tipo di certificato pem con i file PAM.cer e PAM.key

Il seguente esempio di igwCertUtil crea un certificato pem con un file .cer e un file .key.

```
igwCertUtil -version 4.6.0.0
-create -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
      <subject>CN=PAM</subject>
   </Certificate>"
```

### Esempio: creare un tipo di certificato pem per un'autorità di rilascio

Il seguente esempio di igwCertUtil crea un certificato in cui l'autorità di rilascio denominata ha fornito i file issuer.cer e issuer.key.

```
igwCertUtil -version 4.6.0.0
-create -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
      <subject>CN=PAM</subject>
   </Certificate>"
-issuer
   "<Certificate>
      <certType>pem</certType>
      <certURI>issuer.cer</certURI>
      <keyURI>issuer.key</keyURI>
   </Certificate>"
```

### Esempio: copiare PAM.cer con PAM.key in PAM.p12

Nell'esempio seguente, l'utilità igwCertUtil copia il certificato pem nel certificato p12 di destinazione. Il certificato pem include il nome dei file .cer e .key. Il certificato p12 include la combinazione di nome e password.

```
igwCertUtil -version 4.6.0.0
-copy -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

### Esempio: convertire PAM.cer e PAM.key in PAM.p12 e password

Nell'esempio seguente, l'utilità igwCertUtil converte il tipo di certificato pem in un tipo di certificato p12. L'utilità converte PAM.cer in PAM.p12 e PAM.key in una password.

```
igwCertUtil -version 4.6.0.0
-conv -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

## Configurazione delle proprietà di dominio

Il dominio è l'elemento principale nella gerarchia di CA Process Automation. È possibile modificare alcune proprietà di dominio, come la frequenza con cui gli agenti notificano all'orchestrator di dominio che sono attivi. La modifica del valore heartbeat da 2 a 3, ad esempio, può ridurre il traffico di rete. L'impostazione specificata a livello di dominio può essere ereditata o sostituita a livello di ambiente.

**Nota:** Consultare la *Guida di riferimento all'interfaccia utente* per le descrizioni dei campi.

Gli amministratori del contenuto nel gruppo PAMAdmins possono bloccare il dominio e modificarne le proprietà. Le autorizzazioni Domain_Admin nella policy Dominio di CA EEM consentono tali modifiche.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.

   Il riquadro Browser di configurazione viene visualizzato con il nodo Dominio selezionato.

2. Fare clic sulla scheda Proprietà.

3. Visualizzare i campi di sola lettura, ad esempio:

   a. Visualizzare la voce URL di dominio. Questa voce corrisponde alla prima parte dell'URL utilizzato per accedere a CA Process Automation. La voce URL di dominio può identificare l'orchestrator di dominio o l'utilità di bilanciamento del carico. L'URL può indicare se la comunicazione è protetta o di base.

   b. Visualizzare la voce Nome host. Questa voce identifica l'host sul quale è installato l'orchestrator di dominio.

   c. Visualizzare la voce Nome orchestrator. A livello di dominio, questa voce corrisponde all'orchestrator di dominio per impostazione predefinita.

   d. Visualizzare la voce Stato. Lo stato riferito al dominio può avere i valori Attivo o Bloccato da con l'*ID utente*.

4. Con il nodo Dominio selezionato, fare clic su Blocca.

   Quando si blocca il dominio, è possibile modificare solo le proprietà di dominio.

5. Per modificare l'impostazione Intervallo di heartbeat (minuti), scegliere un nuovo valore dalla casella di selezione.

   L'impostazione di un nuovo valore modifica la frequenza con cui gli agenti inviano un heartbeat all'orchestrator di dominio. Per impostazione predefinita, gli agenti inviano un heartbeat ogni 2 minuti. Questa configurazione si applica a tutti gli agenti nel dominio, ma è possibile sostituire questo valore ereditato per qualsiasi agente specifico. Se il valore viene aumentato si riduce il traffico di rete. Aumentare l'intervallo a 1 minuto per identificare i problemi degli agenti più velocemente.

6. Considerare di mantenere a livello di dominio l'impostazione predefinita (Disabilitato) dell'opzione Protezione touchpoint.

   L'impostazione Abilitato specifica di verificare e applicare i diritti utente sulle destinazioni in un dato processo. I diritti utente vengono configurati in una policy personalizzata di CA EEM basata sulla classe di risorsa Protezione touchpoint. È possibile concedere diritti di esecuzione a un utente o un gruppo per un ambiente o un touchpoint specifico.

   **Nota:** consultare la sezione Introduzione alla configurazione di Protezione touchpoint (a pagina 150).

7. Configurare le destinazioni Gruppo host in base alle linee guida seguenti:

   - Disabilitare la proprietà Crea corrispondenza solo nei gruppi host? se i modelli configurati per i gruppi host a volte corrispondono agli indirizzi IP o ai nomi host di:

     - Host con agenti installati che sono associati a touchpoint.
     - Host remoti che sono connessi ad agenti associati a touchpoint proxy.

     **Nota:** In questo caso, l'opzione Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host? per impostazione predefinita.

   - Abilitare la proprietà Crea corrispondenza solo nei gruppi host? se i modelli configurati per i gruppi host a volte corrispondono agli indirizzi IP o ai nomi host di:

     - Host con agenti installati che sono associati a touchpoint.
     - Host remoti che sono connessi ad agenti associati a touchpoint proxy.

   - Disabilitare la proprietà Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host? se i responsabili di progettazione dei contenuti generalmente utilizzano le convenzioni seguenti:

     - Utilizzano un nome host quando il tipo di modello usato nella configurazione Gruppo host è un modello di nome host.
     - Utilizzano un indirizzo IP quando il tipo di modello usato nella configurazione di Gruppo host è una subnet, un intervallo di indirizzo IP o un elenco di indirizzi IP.

   - Abilitare la proprietà Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host? se i responsabili di progettazione dei contenuti si rendono conto che i gruppi host fanno riferimento a host specifici, senza conoscere necessariamente la modalità. Se abilitata, la proprietà assicura che l'operatore riesca a individuare un host di destinazione. Ad esempio, un operatore che specifica l'host come indirizzo IP può trovare la destinazione se Gruppo host fa riferimento ad essa con un modello di nome host.

8. Specificare i requisiti per l'eliminazione definitiva dei dati di reporting che sono stati generati in tale dominio. In alternativa, eliminare in modo definitivo i dati di reporting su richiesta specificando l'intervallo di date in cui i report sono stati generati.

    a. Specificare se eliminare quotidianamente i dati di reporting nel campo Opzione di eliminazione dei dati di reporting. Se si seleziona Elimina dati di reporting tutti i giorni, specificare il momento del giorno in cui avviare l'eliminazione. Ad esempio, per avviare l'eliminazione definitiva alle 6:30 del pomeriggio, specificare l'equivalente nel sistema a 24 ore, ovvero 18:30, nel campo Ora di inizio dell'eliminazione giornaliera dei dati di reporting.

    b. Se è stata specificata una pianificazione per l'eliminazione definitiva, indicare il numero di giorni in cui i dati di reporting devono essere conservati prima dell'eliminazione definitiva. Ad esempio, se si specifica 14 nel campo Numero di giorni di conservazione dei dati di reporting, vengono eliminati tutti i dati di reporting risalenti a più di due settimane fa.

    c. Fare clic sul pulsante Elimina dati di reporting, specificare un intervallo di date relativo ai dati di reporting da eliminare, quindi fare clic su OK.

9. Per generare il reporting per i processi, selezionare la casella di controllo Abilita reporting di processo. Per disabilitare questa funzionalità, deselezionare la casella di controllo Abilita reporting di processo.

10. Per generare i dati di reporting per gli operatori, selezionare la casella di controllo Abilita reporting dell'operatore. Per disabilitare questa funzionalità, deselezionare la casella di controllo Abilita reporting dell'operatore.

11. Per consentire ai responsabili di progettazione dei contenuti di visualizzare i log di processo nell'ambiente di progettazione, selezionare la casella di controllo Abilita log di processo. Per nascondere i log per l'istanza di processo in fase di runtime a livello di ambiente nell'ambiente di produzione, deselezionare la casella di controllo Abilita log di processo.

12. Per automatizzare il ripristino dell'operatore, accettare il valore predefinito per la proprietà Abilita ripristino dell'operatore.

13. Fare clic su Salva.

14. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Blocco del dominio (a pagina 137)
Introduzione alla configurazione di Protezione touchpoint (a pagina 150)
File di proprietà di configurazione Oasis (a pagina 411)

## Introduzione alla configurazione di Protezione touchpoint

Protezione touchpoint è una proprietà a livello di dominio. Per impostazione predefinita, Protezione touchpoint non è applicata. La non applicazione ereditata consente ai processi esistenti di essere eseguiti correttamente.

**Nota:** se si configura Protezione touchpoint come applicata e non è presente alcuna norma Protezione touchpoint in CA EEM, non è in atto alcuna protezione.

In genere, gli host di importanza strategica e gli host che contengono dati estremamente sensibili esistono solo in un ambiente di produzione. Se il proprio dominio di CA Process Automation è stato partizionato in un ambiente di progettazione e un ambiente di produzione, considerare le linee guida seguenti:

- Ambiente di progettazione: accettare le impostazioni ereditate, in cui Protezione touchpoint è disabilitata
- Ambiente di produzione: configurare Protezione touchpoint su Abilitato nelle proprietà di ambiente. Quindi, creare una norma Protezione touchpoint globale che autorizzi l'esecuzione di operatori in categorie selezionate per il gruppo o gli utenti specificati. Specificare Ambiente come filtro. Quindi specificare un filtro per ciascun touchpoint mappato su un host aziendale strategico.

In alternativa, è possibile utilizzare Protezione touchpoint in un ambiente di sviluppo o di test per limitare gli utenti che possono eseguire processi sul proprio orchestrator. In tal caso, si potrebbe creare una norma ed elencare tutti i membri del personale come Identità. In questa norma, si creano due filtri: uno per l'orchestrator come touchpoint e un altro per l'ambiente.

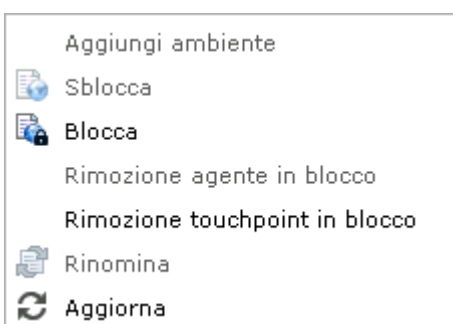
**Ulteriori informazioni:**

Configurazione delle proprietà di dominio (a pagina 147)
Creazione di una policy Protezione touchpoint (a pagina 130)

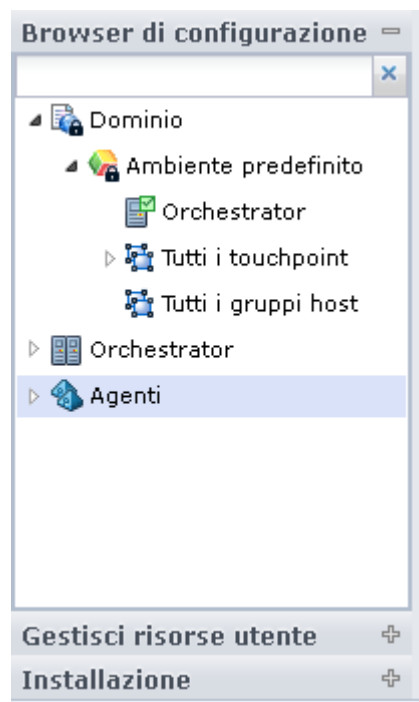
# Gestione della gerarchia di dominio

Per impostazione predefinita, tutti gli amministratori assegnati al gruppo PAMAdmins dispongono delle autorizzazioni Domain_Admin. Se si utilizzano norme e gruppi personalizzati, è possibile limitare le autorizzazioni Domain_Admin ad amministratori selezionati.

Le attività che possono essere eseguite solamente da un utente con autorizzazioni Domain_Admin sono le azioni che richiedono il blocco del dominio. Consultare la sezione Blocco e sblocco del dominio (a pagina 137).

Queste attività modificano la gerarchia di dominio rinominando un nodo oppure aggiungendo o rimuovendo alcuni nodi.

- Aggiunta di un ambiente - consultare la sezione Aggiunta di un ambiente al dominio (a pagina 154).
- Rimozione di un ambiente - consultare la sezione Rimozione di un ambiente da un dominio (a pagina 155).
- Rimozione agente in blocco - consultare la sezione Rimozione degli agenti selezionati in blocco (a pagina 217).
- Rimozione touchpoint in blocco - consultare la sezione Rimozione dei touchpoint vuoti non utilizzati in blocco (a pagina 236).
- Ridenominazione del dominio - consultare la sezione Ridenominazione del dominio (a pagina 156).

# Informazioni su orchestrator, agenti e la gerarchia di dominio

Nel riquadro Browser di configurazione della scheda Configurazione, è presente un oggetto principale che il prodotto denomina Dominio durante l'installazione. Il dominio è l'elemento principale per tutti gli elementi configurabili nel prodotto.

Il Browser di configurazione visualizza le entità fisiche e logiche.

**Entità fisiche**

Un componente *fisico* è un componente installato (un orchestrator o un agente).

**Orchestrator**

**Orchestrator di dominio**

Subito dopo l'installazione, l'orchestrator di dominio è l'unico componente fisico.

**Altri orchestrator**

Gli amministratori possono installare altri orchestrator dal riquadro Installazione.

**Agenti**

Gli amministratori possono installare gli agenti dal riquadro Installazione.

**Operatore logico**

Una o più entità *logiche* comprendono la gerarchia di dominio, formata da uno o più ambienti. Ciascun ambiente dispone di uno o più touchpoint dell'orchestrator e può disporre di touchpoint e gruppi host associati agli agenti.

**Dominio**

Il dominio è il nodo principale nella gerarchia di dominio. Il prodotto dispone di un dominio.

**Ambiente predefinito**

L'ambiente predefinito è l'ambiente creato dal programma di installazione.

**Orchestrator (touchpoint)**

Durante l'installazione, il prodotto visualizza in Ambiente predefinito il touchpoint dell'orchestrator che associa l'orchestrator di dominio all'ambiente predefinito. Ogni orchestrator richiede un touchpoint separato.

**Nota:** Il prodotto associa l'ambiente di un touchpoint dell'orchestrator in cluster al touchpoint per tale cluster. Quando si utilizza un touchpoint di questo tipo come destinazione dell'operatore, l'utilità di bilanciamento del carico seleziona il nodo di destinazione.

**Tutti i touchpoint**

Durante l'installazione, il nodo Tutti i touchpoint è vuoto. Da un agente installato è possibile configurare un touchpoint in un ambiente selezionato. I touchpoint associano gli agenti agli ambienti. Il nodo Tutti i touchpoint in Ambiente predefinito contiene solo i touchpoint associati all'ambiente predefinito. Su un agente possono mappare più touchpoint. Un singolo touchpoint può mappare su più agenti.

**Tutti i gruppi host**

Durante l'installazione, il nodo Tutti i gruppi host è vuoto. Da un agente installato, è possibile creare un gruppo host in un ambiente selezionato e configurare le proprietà del gruppo host. La connettività di un agente a un gruppo di host remoti richiede un account utente su ciascun host remoto. Gli account utente vengono configurati con le credenziali definite nelle proprietà del gruppo host.

**Altro ambiente**

È possibile creare un ambiente di produzione distinto. Ogni ambiente richiede almeno un touchpoint dell'orchestrator.

**Altre voci per orchestrator (touchpoint), Tutti i touchpoint, Tutti i gruppi host nel nuovo ambiente**

Per ciascun orchestrator installato, creare un touchpoint in un ambiente selezionato. I touchpoint dell'orchestrator vengono visualizzati sotto il nodo dell'ambiente selezionato. Tutti i touchpoint agente creati vengono visualizzati in Tutti i touchpoint per tale ambiente. Tutti i gruppi host creati vengono visualizzati in Tutti i gruppi host per tale ambiente.

Gli amministratori del contenuto automatizzano i processi creando e collegando gli operatori. Gli operatori in genere utilizzano come destinazione (per l'esecuzione) un touchpoint dell'orchestrator specifico. Un operatore può utilizzare come destinazione un touchpoint associato a più agenti. In questo caso, quell'operatore può essere potenzialmente eseguito su qualsiasi host agente associato.

## Aggiunta di un ambiente al dominio

Gli amministratori possono aggiungere un ambiente al dominio. In genere, gli amministratori aggiungono un Ambiente di produzione.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.

   Il riquadro presenta l'icona del dominio con un lucchetto, a indicare che è bloccato.

2. Fare di nuovo clic con il pulsante destro del mouse su Dominio e selezionare Aggiungi ambiente.

3. Nella finestra di dialogo Aggiungi nuovo ambiente, immettere un nome per l'ambiente, quindi fare clic su OK.

   Nel riquadro Browser di configurazione è visualizzato il nome del nuovo ambiente con nodi per aggiungere Tutti i touchpoint e Tutti i gruppi host. Inizialmente, il nuovo ambiente non presenta alcun orchestrator.

4. Fare clic su Salva.

5. Selezionare Dominio e fare clic su Sblocca.

## Rimozione di un ambiente dal dominio

Gli utenti con diritti di amministratore di dominio possono eliminare un ambiente dal dominio. Se l'ambiente viene utilizzato attivamente, adottare le misure necessarie per mantenere gli oggetti libreria e le destinazioni di esecuzione.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse su Dominio, quindi fare clic su Blocca.
3. Rivedere gli operatori nei processi attivi che utilizzano come destinazione un orchestrator o touchpoint nell'ambiente di destinazione.
4. Riconfigurare o rimuovere i touchpoint, i touchpoint proxy, i gruppi host e i gruppi touchpoint che sono associati all'ambiente di destinazione. Ad esempio, associare i touchpoint agente a un altro ambiente.
5. Se necessario, spostare il contenuto della libreria in un altro ambiente.

   **Nota:** gli argomenti seguenti descrivono le procedure da seguire per spostare i contenuti:

   - Esportazione di una cartella (a pagina 363)
   - Importazione di una cartella (a pagina 364)
6. Rimuovere tutti gli orchestrator dall'ambiente:
   a. Mettere in quarantena l'orchestrator (a pagina 194).
   b. Rimuovere l'orchestrator dall'ambiente (a pagina 169).
7. Fare clic con il pulsante destro del mouse sull'ambiente, quindi selezionare Elimina.
8. Fare clic su Sì nel messaggio di conferma.
9. Fare clic su Salva.
10. Selezionare Dominio e fare clic su Sblocca.

## Ridenominazione del dominio

Nella documentazione e nella Guida in linea il nome dominio viene utilizzato per fare riferimento al dominio di CA Process Automation. Gli amministratori con autorizzazioni Domain_Admin possono rinominare questo nodo superiore della gerarchia di dominio.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Selezionare Dominio e fare clic su Blocca.
3. Fare clic con il tasto destro del mouse su Dominio, quindi selezionare Rinomina.
4. Inserire il nuovo nome nel campo che contiene il dominio.
5. Fare clic su Salva.
6. Selezionare Dominio e fare clic su Sblocca.

# Capitolo 6: Amministrazione degli ambienti

Al momento dell'installazione, il dominio di CA Process Automation dominio dispone di un solo ambiente, quello predefinito. Gli amministratori definiti nel gruppo di PAMAdmins predefinito hanno tutti i diritti. È possibile creare norme di CA EEM che concedono diritti di amministratore specifici a utenti differenti. Ad esempio:

- Un amministratore con diritti di *amministratore di dominio* può creare altri ambienti per suddividere il dominio. In genere, l'ambiente predefinito viene utilizzato per progettare processi automatizzati e supportare gli oggetti. Quando uno o più processi sono pronti per l'uso nell'ambiente di produzione esistente, l'amministratore crea un ambiente in CA Process Automation e lo chiama ambiente di produzione. Altri esempi includono segmentazione geografica, basata sui cicli di vita o sulle varie fasi. In questo capitolo verranno trattate tali attività.
- Un amministratore con diritti di *amministratore del contenuto di ambiente* può aggiungere touchpoint e gruppi host, creare gruppi touchpoint, nonché rimuovere in blocco i touchpoint inutilizzati. Può inoltre creare nuovi oggetti, compresi processi e pianificazioni. Consultare i capitoli successivi per ulteriori informazioni su touchpoint e gruppi host. Consultare la *Guida alla progettazione dei contenuti* per ulteriori informazioni sull'utilizzo delle schede Libreria e Progettazione per la creazione e lo sviluppo dei contenuti.
- Un amministratore con diritti di *amministratore della configurazione di ambiente* può configurare i contenuti di un ambiente selezionato. Gli amministratori possono accettare o sovrascrivere le impostazioni ereditate. La configurazione dei contenuti di un ambiente può includere la modifica delle impostazioni di protezione, l'impostazione delle proprietà ambientali, l'abilitazione o disabilitazione delle categorie di operatori e l'eredità di impostazioni per i trigger.

Questa sezione contiene i seguenti argomenti:



## Configurazione dei contenuti di un ambiente

Quando si seleziona un ambiente nel browser di configurazione, le schede seguenti vengono visualizzate nei contenuti di <environment name>:

- Protezione

  Consultare la sezione Visualizzazione o ripristino delle impostazioni di protezione per un ambiente selezionato (a pagina 158).

- Ammissione automatica

  Consultare la sezione Aggiunta di touchpoint in blocco per gli agenti (a pagina 233).

- Proprietà

  Consultare la sezione Configurazione delle proprietà dell'ambiente (a pagina 159).

- moduli

  Consultare la sezione Abilitazione di una categoria operatore e sovrascrittura delle impostazioni ereditate (a pagina 163).

- trigger

  Consultare la sezione Specificazione delle impostazioni dei trigger per un ambiente (a pagina 164).

- Audit trail

  Consultare la sezione Visualizzazione dell'audit trail per un ambiente (a pagina 346).

## Visualizzazione o ripristino delle impostazioni di protezione per un ambiente selezionato

La maggior parte delle impostazioni della scheda Protezione vengono create durante l'installazione o l'aggiornamento dell'orchestrator di dominio. È possibile modificare le impostazioni di sola lettura solo reinstallando l'orchestrator di dominio.

Ciascun ambiente eredita le impostazioni stabilite durante l'installazione dell'orchestrator di dominio. Se la casella di controllo Eredita viene deselezionata, è possibile aggiornare l'Intervallo di aggiornamento della cache CA EEM (in secondi). Se si riduce l'intervallo di aggiornamento, CA Process Automation riflette le modifiche apportate in CA EEM più velocemente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere Dominio nel riquadro Browser di configurazione e selezionare l'ambiente di destinazione.

   Viene visualizzata la scheda Protezione.

3. Esaminare le impostazioni di protezione stabilite durante il processo di installazione.

4. (Facoltativo) Aggiornare il valore Intervallo di aggiornamento della cache CA EEM.
    a. Fare clic su Blocca.
    b. Deselezionare la casella di controllo Eredita.
    c. Aggiornare il valore.
    d. Fare clic su Salva.
    e. Selezionare l'ambiente e fare clic su Sblocca.

    **Nota:** Se l'intervallo di aggiornamento della cache di CA EEM è stato ridotto, considerare l'eliminazione della cache per le autorizzazioni di CA Process Automation. Consultare la sezione Controllo delle cache per gli aggiornamenti di CA EEM (a pagina 78).

**Ulteriori informazioni:**

Configurazione delle impostazioni di protezione di CA EEM per il dominio (a pagina 140)

## Configurazione delle proprietà dell'ambiente

Configurare le proprietà di un ambiente selezionato dalla scheda Configurazione. Per poter configurare le proprietà dell'ambiente o sostituire le impostazioni ereditate dall'ambiente, è necessario disporre dei diritti Amministratore della configurazione di ambiente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo Dominio, fare clic con il pulsante destro del mouse sul nome dell'ambiente appropriato, quindi fare clic su Blocca.

3. Fare clic sulla scheda Proprietà, quindi visualizzare o aggiornare le proprietà se necessario.

   **Ripristino automatico operatori**

   Specifica se il ripristino viene eseguito in modo automatico. Il ripristino si applica a operatori specifici non riusciti con SYSTEM_ERROR i cui processi recuperabili sono in stato BLOCCATO, IN ESECUZIONE o IN ATTESA. Selezionare True per iniziare il ripristino quando l'orchestrator o l'agente non attivo diventa attivo. Il ripristino reimposta operatori che erano in SYSTEM_ERROR e riprende i relativi processi. Gli operatori reimpostati in un processo ripreso cominciano a essere eseguiti sulle destinazioni associate. Le destinazioni degli operatori possono essere orchestrator, touchpoint, host connessi a touchpoint proxy o host in un gruppo host.

   **Valori:** questa proprietà presenta i valori seguenti:

   - **Opzione selezionata**: il ripristino automatico è abilitato.
   - **Opzione deselezionata**: il ripristino automatico è disabilitato.

   **Impostazione predefinita:** opzione selezionata.

   **Protezione touchpoint**

   Specifica se ereditare il valore configurato nelle proprietà di dominio o se impostare il valore su True o False a livello di ambiente.

   **Valori:** questa proprietà presenta i valori seguenti:

   - **Eredita dal dominio**: utilizzare il valore configurato per questo campo nelle proprietà del dominio.
   - **Abilitato**: si attuano le policy Protezione touchpoint per questa destinazione e si consente l'accesso solo se l'utente dispone di questa autorizzazione.
   - **Disabilitato**: non si verifica se l'utente che esegue il processo dispone dei diritti di esecuzione sulla destinazione corrente.

   **Impostazione predefinita:** Eredita dal dominio.

**Crea corrispondenza solo nei gruppi host?**

Specifica l'ambito di ricerca per una destinazione dell'operatore quando la voce di campo Destinazione è un indirizzo IP o un nome host (FQDN). È possibile procedere con l'esecuzione dell'operatore sulla destinazione solo quando quest'ultima è nota a CA Process Automation. Selezionare Disabilitato per avviare una ricerca più ampia. Selezionare Abilitato qui e Disabilitato nel campo successivo per una ricerca più limitata.

**Nota:** Una ricerca DNS di un nome host specificato consente di individuare gli indirizzi IP associati, mentre una ricerca DNS dell'indirizzo IP consente di individuare i nomi host associati.

**Valori:** questa proprietà presenta i valori seguenti:

- **Eredita dal dominio**: utilizzare il valore configurato per questo campo nelle proprietà del dominio.
- **Abilitato**: l'ambito della ricerca dipende a seconda se il campo Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host? è abilitato o disabilitato.

  Se la ricerca DNS è disabilitata, viene cercato: il riferimento di gruppo host a un host remoto (esatto)

  Se la ricerca DNS è abilitata, viene cercato: il riferimento di gruppo host a un host remoto (esatto o risultato di ricerca DNS)
- **Disabilitato**: i componenti di dominio vengono cercati nell'ordine seguente:

  Touchpoint (esatto o risultato di ricerca DNS)

  Orchestrator (esatto o risultato di ricerca DNS)

  Agente (esatto o risultato di ricerca DNS)

  Touchpoint proxy con mapping su un host remoto (esatto o risultato di ricerca DNS)

  Il riferimento di gruppo host a un host remoto (esatto o risultato di ricerca DNS)

**Impostazione predefinita:** Eredita dal dominio.

**Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host?**

**Nota:** Questo campo viene abilitato quando l'opzione Crea corrispondenza solo nei gruppi host è impostata su Abilitato.

Specifica se limitare la ricerca tramite i riferimenti di gruppo host al tipo di voce. Ad esempio, quando il tipo di voce del campo Destinazione è un FQDN, cercare solamente modelli di nome host. Quando il tipo di voce di campo Destinazione è un indirizzo IP, cercare solo le subnet. Quando viene inclusa una ricerca DNS, si può accettare anche un riferimento di gruppo host per l'altro tipo, come risolto da una ricerca DNS.

**Valori:** questa proprietà presenta i valori seguenti:

- **Eredita dal dominio**: utilizzare il valore configurato per questo campo nelle proprietà del dominio.
- **Abilitato**: vengono cercati tutti i riferimenti di gruppo host. I riferimenti di gruppo host per nomi host sono modelli (espressioni regolari) che possono includere il nome host specificato. I riferimenti di gruppo host per gli indirizzi IP sono subnet di indirizzo IP espresse in notazione CIDR che possono includere l'indirizzo IP specificato. Estendere la ricerca a tutti i riferimenti di gruppo host. Eseguire la ricerca per trovare una corrispondenza esatta o una corrispondenza con il risultato di ricerca DNS.
- **Disabilitato**: si limita la ricerca ai riferimenti di gruppo host che includono una corrispondenza esatta con la voce del campo Destinazione.

**Impostazione predefinita:** Eredita dal dominio.

4. Fare clic su Salva.
5. Selezionare l'ambiente e fare clic su Sblocca.

   Gli aggiornamenti delle proprietà di ambiente sono attivi.

**Ulteriori informazioni:**

Introduzione alla configurazione di Protezione touchpoint (a pagina 150)
Personalizzazione della categoria operatore per un agente selezionato (a pagina 210)

## Abilitazione di una categoria operatore e sovrascrittura delle impostazioni ereditate.

Per impostazione predefinita, le impostazioni delle categoria operatore vengono visualizzate in un ambiente come Eredita dal dominio. Quando le impostazioni delle categoria operatore vengono configurate al livello di Dominio, un amministratore può accettare le impostazioni ereditate. Un amministratore con diritti di amministratore della configurazione di ambiente può abilitare qualsiasi categoria operatore e sostituire le impostazioni ereditate a livello di ambiente.

Per esaminare le impostazioni per qualsiasi categoria operatore, è necessario abilitare la categoria.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio, selezionare un ambiente e fare clic su Blocca.
3. Fare clic sulla scheda Moduli.
4. Per visualizzare le impostazioni per qualsiasi categoria operatore, fare clic su Eredita dal dominio e selezionare Abilita dall'elenco a discesa.
5. Fare clic con il pulsante destro del mouse sulla categoria operatore e selezionare Modifica.

   Le impostazioni correnti vengono visualizzate.
6. Facoltativamente, configurare impostazioni per uno o più campi.

   **Nota:** consultare la sezione Configurazione di categorie operatori (a pagina 276) per dettagli a livello di campo.
7. Fare clic su Salva.
8. Fare clic su Chiudi.
9. Fare clic con il pulsante destro del mouse sull'ambiente e selezionare Sblocca.

**Ulteriori informazioni:**

Configurazione di Utilità di rete (a pagina 306)
Configurazione di Servizi Web (a pagina 311)
Configurazione di Controllo processo (a pagina 308)
Configurazione di Gestione file (a pagina 302)
Configurazione di Esecuzione comando: Proprietà Telnet predefinite (a pagina 283)

## Specificazione delle impostazioni dei trigger per un ambiente

Le impostazioni dei trigger sono disabilitate a livello di ambiente per impostazione predefinita. Se le impostazioni dei trigger sono state configurate a livello di dominio, è possibile specificare che si desidera ereditare tali impostazioni. In alternativa, è possibile abilitare un trigger, quindi sostituire le impostazioni a livello di dominio. Se necessario, è possibile disabilitare un trigger che è abilitato o impostato per ereditare i valori.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Rivedere le impostazioni a livello di dominio per il trigger:
   a. Fare clic su Dominio
   b. Fare clic sulla scheda Trigger.
   c. Fare doppio clic su un trigger.
   d. Determinare se il trigger è stato configurato, e in tal caso, se accettare le impostazioni per un determinato ambiente.
3. Selezionare un ambiente e fare clic su Blocca.
4. Fare clic sulla scheda Trigger.
5. Selezionare un trigger.
6. Selezionare un nuovo valore dall'elenco a discesa.

   **Eredita dal dominio**

   Specifica che le impostazioni configurate a livello di dominio vengono utilizzate nell'ambiente selezionato.

   **Disattivato**

   Specifica che il trigger non viene utilizzato nell'ambiente.

   **Attivato**

   Specifica che il trigger deve utilizzare le impostazioni configurate per l'ambiente.

7. Se Abilitato è selezionato, fare clic con il tasto destro del mouse sul trigger e selezionare Modifica. Modificare le impostazioni utilizzando le informazioni seguenti come guida:
   - Configurazione delle proprietà di trigger di file a livello di dominio (a pagina 329).
   - Configurazione delle proprietà di trigger di posta a livello di dominio (a pagina 330).
   - Configurazione delle proprietà di trigger di SNMP a livello di dominio (a pagina 334).

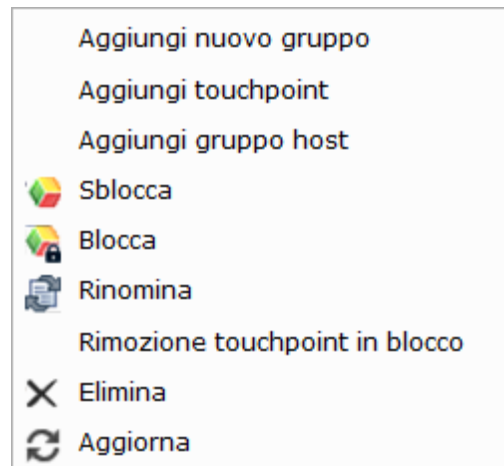
- Configurazione delle proprietà di trigger Catalyst a livello di dominio (a pagina 326).

8. Fare clic su Salva.
9. Fare clic su Chiudi.
10. Selezionare l'ambiente aggiornato e fare clic su Sblocca.

# Aggiornamento della gerarchia di un ambiente

La gerarchia di dominio è composta da uno o più ambienti, in cui ciascun ambiente presenta almeno un orchestrator e uno o più touchpoint che associano l'ambiente a un agente. Quando un operatore in un processo in esecuzione utilizza come destinazione un touchpoint, l'operatore viene eseguito sull'agente o sull'orchestrator associato al touchpoint. Quando un operatore utilizza come destinazione un gruppo touchpoint, esso viene eseguito su tutti gli agenti e gli orchestrator associati.

Per supportare l'esecuzione degli operatori sugli host remoti, cioè host privi di agente, un ambiente può includere touchpoint proxy e gruppi host. Un touchpoint proxy associa un host remoto a un agente; un gruppo host associa diversi host remoti a un agente. In entrambi i casi l'host agente si connette all'host remoto mediante una connessione SSH attendibile.

Un amministratore che dispone delle autorizzazioni Environment_Configuration_Admin (amministratore di configurazione) può aggiornare la gerarchia di un ambiente selezionato. Le opzioni di menu per un ambiente, selezionabili facendo clic con il tasto destro del mouse, sono le seguenti:

Seguono i collegamenti agli argomenti delle opzioni del menu Ambiente:

- Aggiungi Nuovo gruppo

  Consultare la sezione Raggruppamento di touchpoint in un ambiente (a pagina 239).

- Aggiungi touchpoint

  Consultare la sezione Aggiunta di un touchpoint e creazione di un'associazione (a pagina 230) e i capitoli Amministrazione dei touchpoint e Amministrazione di touchpoint proxy per ulteriori informazioni.

  Consultare anche la sezione Aggiunta di un orchestrator a un ambiente (a pagina 168).

- Aggiungi gruppo host

  Consultare la sezione Creazione di un gruppo host (a pagina 256) e il capitolo Amministrazione di gruppi host per ulteriori informazioni.

- Rinomina

  Consultare la sezione Rinominare un ambiente (a pagina 167).

- Rimozione globale dei touchpoint

  Consultare la sezione Rimozione in blocco dei touchpoint vuoti inutilizzati (a pagina 236).

- Elimina - Può essere utilizzata per rimuovere eventuali oggetti logici aggiunti dall'utente dalla gerarchia di dominio, ovvero:

  - Qualsiasi ambiente.
  - Qualsiasi touchpoint dell'orchestrator.

    Consultare la sezione Eliminazione di un touchpoint dell'orchestrator (a pagina 169).

  - Qualsiasi touchpoint agente.
  - Qualsiasi gruppo touchpoint.
  - Qualsiasi gruppo host.

## Rinominare un ambiente

Gli amministratori che dispongono dei diritti Environment_Configuration_ Admin (amministratore di configurazione) possono rinominare un ambiente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.

   Viene visualizzato il riquadro Browser di configurazione.

2. Fare clic con il tasto destro del mouse sul dominio, quindi fare clic su Blocca.
3. Fare clic con il pulsante destro del mouse sull'ambiente, quindi fare clic su Blocca.
4. Fare clic con il pulsante destro del mouse sull'ambiente e selezionare Rinomina.
5. Immettere un nuovo nome per l'ambiente.
6. Fare clic su Salva.
7. Fare clic con il tasto destro del mouse sul dominio, quindi fare clic su Sblocca.

## Aggiunta di un orchestrator ad un ambiente

Durante l'installazione iniziale di CA Process Automation, l'orchestrator di dominio viene installato nell'ambiente predefinito. L'ambiente predefinito viene in genere utilizzato per le fasi di progettazione e verifica. In genere, gli amministratori creano un ambiente distinto per la produzione.

Ciascun ambiente deve avere almeno un orchestrator, ma qualsiasi ambiente può avere più orchestrator. Ciascun nuovo orchestrator implica un'installazione separata. Dopo avere installato un orchestrator separato, aggiungere tale orchestrator a un ambiente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse sull'ambiente da configurare, quindi fare clic su Blocca.
3. Fare nuovamente clic con il pulsante destro del mouse sull'ambiente, quindi fare clic su Aggiungi touchpoint.

   Viene visualizzata la finestra di dialogo Aggiungi touchpoint.
4. Accanto a Nome touchpoint, immettere un nome per il nuovo orchestrator.
5. Accanto a Selezionare l'agente/orchestrator, fare clic su Orchestrator.

   L'opzione Orchestrator non è disponibile se tutti gli orchestrator del dominio sono già associati a touchpoint esistenti.
6. Nell'elenco degli orchestrator disponibili, selezionare quello al quale si desidera associare il nuovo touchpoint.
7. Fare clic su Salva per aggiungere il nuovo touchpoint all'ambiente.
8. Selezionare il riquadro Browser, fare clic con il pulsante destro del mouse sull'ambiente, quindi fare clic su Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che chiede se si desidera salvare le modifiche.
9. Fare clic su Sì.

   **Nota:** per salvare l'elemento, è possibile anche utilizzare Salva nella parte superiore dello schermo oppure il menu File, senza sbloccarlo.

**Ulteriori informazioni:**

Aggiunta di un touchpoint a un orchestrator (a pagina 179)

## Eliminazione di un touchpoint dell'orchestrator

Un touchpoint dell'orchestrator è un'entità logica che associa un orchestrator selezionato, o la sua utilità di bilanciamento del carico, con un ambiente specifico. Eliminando un touchpoint dell'orchestrator viene rimossa l'associazione, ma l'ambiente o l'orchestrator non sono influenzati. Tuttavia non è possibile accedere a un orchestrator fisico senza touchpoint. Non può accettare richieste da parte di operatori o aggiornamenti della libreria.

È possibile eliminare un touchpoint dell'orchestrator in preparazione della creazione di un nuovo touchpoint per tale orchestrator. È possibile eliminare un touchpoint dell'orchestrator in preparazione del ritiro di tale orchestrator.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo di dominio e il nodo dell'ambiente con l'orchestrator da rimuovere.
3. Fare clic con il tasto destro del mouse sul dominio, quindi fare clic su Blocca.
4. Fare clic con il pulsante destro del mouse sull'ambiente contenente l'orchestrator che si desidera eliminare, quindi fare clic su Blocca.
5. Fare clic con il tasto destro del mouse sull'orchestrator che si desidera eliminare, e selezionare Elimina.
6. Fare clic su OK per confermare l'eliminazione dell'orchestrator.
7. Fare clic con il pulsante destro del mouse sull'ambiente, quindi fare clic su Sblocca.
8. Fare clic con il tasto destro del mouse sul dominio e fare clic su Sblocca.

   Il touchpoint di orchestrator viene eliminato.

**Ulteriori informazioni:**

Messa in quarantena di un orchestrator (a pagina 194)
Disabilitazione di un touchpoint di orchestrator (a pagina 181)

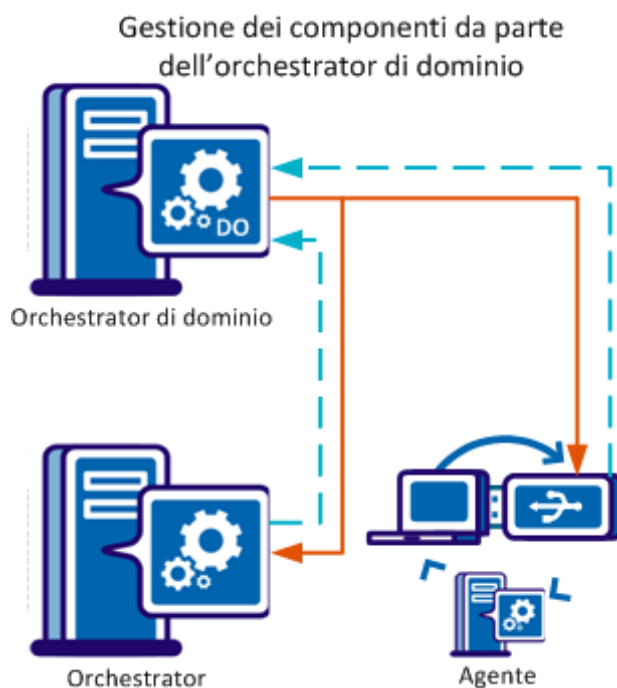
# Capitolo 7: Amministrazione di orchestrator

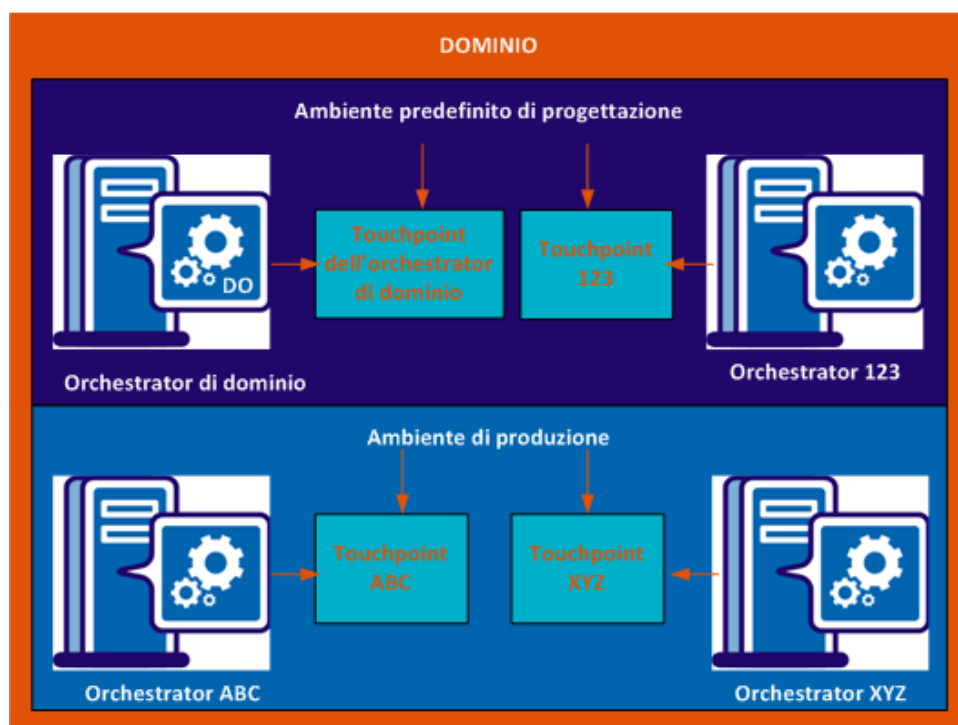
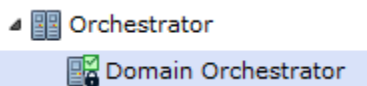
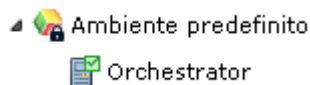
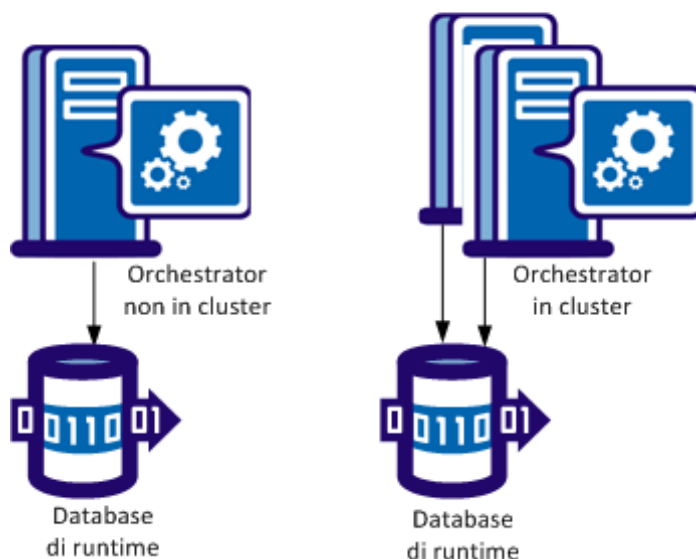
È possibile installare un numero illimitato di orchestrator. La prima installazione crea l'orchestrator di dominio. Quando l'orchestrator di dominio è in esecuzione, è possibile installare altri orchestrator dal riquadro Installazione della scheda Configurazione.

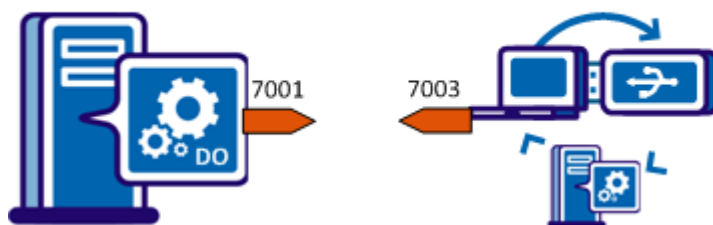
Gli orchestrator sono i moduli di CA Process Automation; elaborano il contenuto progettato con CA Process Automation. Tutti i processi vengono eseguiti sull'orchestrator, i quali gestiscono ed eseguono oggetti di automazione. Gli orchestrator dirigono gli agenti per l'esecuzione di azioni richieste come parte del processo.

Questa sezione contiene i seguenti argomenti:

# Informazioni sugli orchestrator

L'orchestrator di dominio mantiene la configurazione e lo stato di tutti i componenti del dominio. È possibile caricare gli aggiornamenti degli orchestrator o degli agenti sull'orchestrator di dominio. L'orchestrator di dominio invia gli aggiornamenti caricati su tutti gli orchestrator o agenti. Tutti gli orchestrator e gli agenti del Dominio inviano il loro stato all'orchestrator di dominio a intervalli regolari.

Per aggiungere un orchestrator a un ambiente, configurare un touchpoint per l'orchestrator selezionato nell'ambiente specificato. Ciascun orchestrator partecipa a un solo ambiente CA Process Automation. Ogni orchestrator è associato a un solo touchpoint. Se è necessario eseguire un operatore su un touchpoint dell'orchestrator, il campo Destinazione viene lasciato vuoto. Il campo Destinazione non compilato indica di eseguire l'operatore sull'orchestrator di avvio del processo.

Associazione di un orchestrator a un ambiente da parte del touchpoint dell'orchestrator

Vengono configurate le impostazioni specifiche dell'host e vengono visualizzate le informazioni fisiche relative a un orchestrator compreso nel nodo Orchestrator.

Vengono configurate le impostazioni specifiche del touchpoint per lo stesso orchestrator nel nodo Ambiente. È possibile visualizzare le informazioni logiche relative a un orchestrator nell'ambiente corrispondente.

Gli orchestrator possono essere *raggruppati in cluster* (con più nodi) per la disponibilità elevata e la scalabilità o *non raggruppati in cluster* (con un nodo singolo*)*. Un orchestrator in cluster agisce come un singolo orchestrator. Ad esempio, mentre ciascun orchestrator non cluster dispone del proprio database di runtime, gli orchestrator di un nodo cluster condividono un database di runtime comune.

Un processo che viene eseguito su un orchestrator può eseguire un processo secondario su un orchestrator distinto. Un agente può eseguire operazioni in un processo, come ad esempio l'esecuzione di uno script. Gli orchestrator e gli agenti utilizzano una coppia di porte per la comunicazione.

Con la comunicazione non più in uso la porta predefinita dell'orchestrator è 7001. La porta predefinita per gli agenti è 7003. Le porte 7001 e 7003 sono entrambe bidirezionali, ossia inviano e ricevono dati.

Con le comunicazioni semplificate, gli agenti avviano una connessione con socket Web persistente che l'agente e l'orchestrator utilizzano per la comunicazione.

Quando l'orchestrator richiede che un agente completi un'operazione, l'agente restituisce i risultati dell'operazione all'orchestrator. In un'installazione cluster, un nodo di orchestrator invia una richiesta a un agente. L'agente invia il risultato a qualsiasi nodo dell'orchestrator richiedente. Uno dei nodi cluster riceve il risultato dell'agente da una coda condivisa.

**Ulteriori informazioni:**

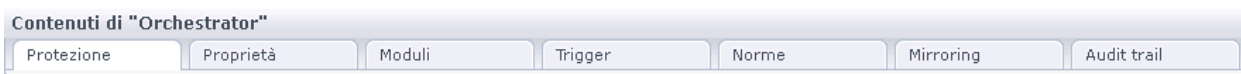
Caricamento Risorse agente (a pagina 341)
Caricamento Risorse orchestrator (a pagina 339)

# Configurazione dei contenuti di un touchpoint dell'orchestrator

Per configurare un touchpoint dell'orchestrator, selezionare l'orchestrator in un nodo Ambiente. Tutte le impostazioni, ad eccezione di una, sono di sola visualizzazione.

Per configurare le impostazioni relative all'host dell'orchestrator, selezionare l'orchestrator nel nodo Orchestrator.

**Nota:** per ulteriori informazioni sulla configurazione consultare la sezione Configurazione dei contenuti di un host dell'orchestrator (a pagina 182).

Seguono le schede per i contenuti dell'orchestrator selezionato:

L'unico campo configurabile in questo insieme di schede è quello per la protezione touchpoint. Nella scheda Proprietà, impostare Protezione touchpoint su True solo dopo aver configurato una norma Protezione touchpoint.

Seguono gli argomenti delle schede orchestrator:

- Protezione: le impostazioni per la protezione non vengono applicate al touchpoint dell'orchestrator. I campi della visualizzazione del touchpoint dell'orchestrator sono disponibili in sola lettura.
- Proprietà: è possibile configurare le proprietà del touchpoint dell'orchestrator (a pagina 176).
- Moduli: le categorie operatore non sono configurabili da un touchpoint dell'orchestrator. È possibile modificare le impostazioni selezionando l'host dell'orchestrator.
- Trigger: i trigger non sono configurabili da un touchpoint dell'orchestrator. È possibile modificare le impostazioni selezionando l'host dell'orchestrator.
- Norme: le nome non sono configurabili da un touchpoint dell'orchestrator. È possibile modificare le impostazioni selezionando l'host dell'orchestrator.
- Mirroring: il mirroring non è configurabile da un touchpoint dell'orchestrator. È possibile modificare le impostazioni relative al mirroring selezionando l'host dell'orchestrator corrispondente.
- Audit trail: le azioni audit trail non si applicano ai touchpoint dell'orchestrator. È possibile visualizzare le azioni controllate sull'host dell'orchestrator corrispondente.

## Configurazione delle proprietà Touchpoint dell'orchestrator

Il riquadro Proprietà del touchpoint dell'orchestrator fornisce informazioni sul touchpoint associato all'orchestrator. È possibile visualizzare informazioni relative allo stato e modificare la configurazione di Protezione touchpoint per questo touchpoint dell'orchestrator.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio e l'ambiente con il touchpoint dell'orchestrator.
3. Selezionare il touchpoint dell'orchestrator da configurare e fare clic su Blocca.
4. Fare clic sulla scheda Proprietà.
5. (Facoltativo) Configurare l'impostazione Protezione touchpoint. Specificare se ereditare l'impostazione o impostare il valore a livello di orchestrator. Quando sono abilitati, i processi utilizzano le policy Protezione touchpoint per autorizzare gli utenti all'esecuzione degli operatori in un processo.

6. Configurare le impostazioni predefinite relative al modo in cui gli operatori elaborano un indirizzo IP o un nome host nel campo Destinazione o se usati come riferimento da un set di dati.

   a. Selezionando l'elenco a discesa Crea corrispondenza solo nei gruppi host? specifica l'ambito di ricerca per una destinazione dell'operatore quando la voce di campo Destinazione è un indirizzo IP o un nome host (FQDN). È possibile procedere con l'esecuzione dell'operatore sulla destinazione solo quando quest'ultima è nota a CA Process Automation.

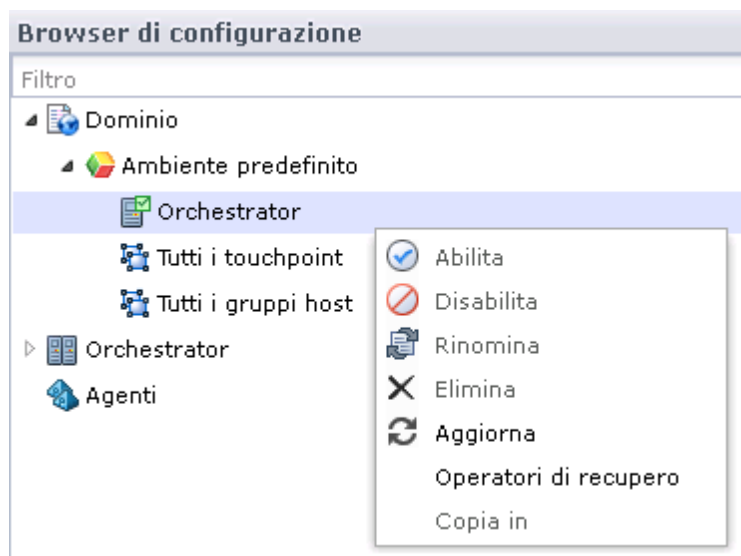
      - Selezionare Disabilitato per avviare una ricerca più ampia.
      - Selezionare Abilitato qui e Disabilitato nel campo successivo per una ricerca più limitata.

   b. Quando è abilitato l'elenco a discesa Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host? si specifica se limitare la ricerca tramite i riferimenti di gruppo host al tipo di voce.

      - Selezionare Abilitato per cercare tutti i riferimenti di gruppo host.
      - Selezionare Disabilitato per limitare la ricerca ai riferimenti di gruppo host che includono una corrispondenza esatta con la voce del campo Destinazione.

7. Fare clic su Salva.
8. Selezionare l'orchestrator e fare clic su Sblocca.
9. Visualizzare le proprietà disponibili. Per ulteriori informazioni, consultare le descrizioni comando.

# Aggiornamento della gerarchia di un touchpoint dell'orchestrator

Quando si seleziona un Orchestrator in Dominio o Ambiente, le informazioni visualizzate sono relative al touchpoint mappato su quell'orchestrator.

Fare riferimento alle seguenti informazioni:

- Abilita: fare clic con il tasto destro del mouse su un touchpoint dell'orchestrator disabilitato e selezionare Abilita.
- Disattiva

  Consultare la sezione Disabilitazione di un touchpoint di orchestrator (a pagina 181).
- Rinomina - specificare un nuovo nome per il touchpoint dell'orchestrator.
- Elimina - fare clic con il pulsante destro del mouse su un touchpoint di Orchestrator e selezionare Elimina. Solo il touchpoint viene eliminato.
- Recover Operators (Ripristina operatori)

  Consultare la sezione Ripristino degli operatori sull'orchestrator di destinazione (a pagina 179).
- Copia in

  Consultare la sezione Creazione di un gruppo touchpoint con i touchpoint selezionati (a pagina 241)

## Aggiunta di un touchpoint a un orchestrator

Quando si aggiunge un orchestrator autonomo a un ambiente, aggiungere un touchpoint all'ambiente ed eseguire il mapping dell'orchestrator. Ogni orchestrator deve essere associato al proprio touchpoint.

Quando si aggiungono i nodi per creare un orchestrator in cluster, l'utilità di bilanciamento del carico utilizza il touchpoint definito per il primo nodo. L'utilità di bilanciamento del carico determina quale nodo deve gestire una richiesta che utilizza come destinazione il touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse sull'ambiente in cui si desidera aggiungere un touchpoint e fare clic su Blocca.
3. Espandere il nodo Orchestrator.
4. Fare clic con il pulsante destro del mouse sull'orchestrator di destinazione, selezionare Configura touchpoint su e fare clic sul nome dell'ambiente bloccato.
5. Nella finestra di dialogo Aggiungi touchpoint dell'orchestrator, immettere un nome per il nuovo touchpoint e fare clic su Aggiungi.
6. Fare clic con il pulsante destro sull'ambiente in cui è stato aggiunto il touchpoint e selezionare Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che richiede se salvare le modifiche.
7. Fare clic su Sì.

   Un nuovo touchpoint dell'orchestrator viene aggiunto all'ambiente selezionato.

**Ulteriori informazioni:**

Aggiunta di un orchestrator ad un ambiente (a pagina 168)

## Ripristino degli operatori sull'orchestrator di destinazione

Il ripristino manuale è sempre abilitato. È possibile richiamare gli operatori di recupero se Ripristino automatico operatori a livello di destinazione è impostato su True, False o Eredita dall'ambiente. Il ripristino degli operatori è appropriato quando un processo si trova nello stato BLOCCATO, IN ESECUZIONE o IN ATTESA e un operatore nel processo non è stato eseguito correttamente restituendo un errore di sistema. Il ripristino degli operatori consente di reimpostare l'operatore e di riprendere il processo.

È possibile richiamare il ripristino di operatore dalla scheda Configurazione quando:

- L'orchestrator prima inattivo diventa attivo. Un orchestrator attivo viene visualizzato in verde.
- L'orchestrator di destinazione è abilitato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio e un ambiente in cui un orchestrator presenta uno o più processi impostati come ripristinabili.
3. Fare clic con il pulsante destro del mouse su Orchestrator e selezionare Aggiorna.
4. Fare clic con il pulsante destro del mouse su Orchestrator e selezionare Operatori di recupero.

   Il ripristino dell'operatore ha inizio.

## Disabilitazione di un touchpoint di orchestrator

Disabilitare un touchpoint di Orchestrator per impedire l'esecuzione di processi su di esso. La disabilitazione di un touchpoint di Orchestrator non ha effetto sulla libreria di Orchestrator. Ciò significa che i responsabili di progettazione dei contenuti possono selezionare un Orchestrator con un touchpoint disabilitato sulla scheda Libreria e possono definire oggetti di automazione.

Disabilitare i touchpoint di orchestrator quando gli oggetti esterni interessati non sono disponibili. Considerare l'esempio di processi che hanno a che fare con il service desk o con un database esterno. A intervalli, questi componenti non sono disponibili per operazioni di manutenzione. È possibile impedire l'esecuzione dei processi che interagiscono con i componenti temporaneamente non disponibili. Quando i componenti esterni diventano disponibili, si abilita il touchpoint di orchestrator. Quindi, l'esecuzione dei processi pianificati che utilizzano questi componenti esterni può essere ripresa.

È possibile disabilitare il touchpoint di orchestrator selezionato nella gerarchia di dominio.

**Attenersi alla procedura seguente:**

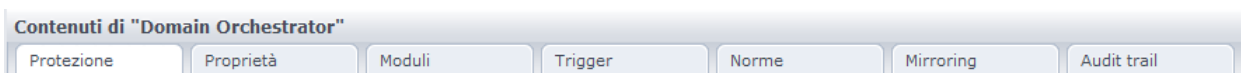
1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo Dominio. Espandere il nodo di ambiente con il touchpoint dell'orchestrator da disattivare.
3. Selezionare un ambiente e fare clic su Blocca.
4. Selezionare il touchpoint dell'orchestrator e fare clic su Blocca.
5. Fare clic con il pulsante destro del mouse sul touchpoint dell'orchestrator e selezionare Disabilita.
6. Fare clic su Sblocca.
7. Selezionare l'ambiente bloccato e fare clic su Sblocca.

**Ulteriori informazioni:**

Messa in quarantena di un orchestrator (a pagina 194)

# Configurazione dei contenuti di un host dell'orchestrator

I dettagli di configurazione che sono univoci per gli orchestrator e che non vengono ereditati includono le norme e il mirroring; tutti i campi di entrambi presentano valori predefiniti. Il mirroring si applica agli orchestrator diversi dall'orchestrator di dominio. Le impostazioni per gli elementi seguenti vengono ereditate per impostazione predefinita: protezione, proprietà, moduli e trigger. Le impostazioni configurate per un host dell'orchestrator sono diverse da quelle configurate sul touchpoint dell'orchestrator.

Di seguito si riportano le schede del menu Orchestrator Host (Host dell'orchestrator):

- Protezione

  Consultare la sezione Visualizzazione delle impostazioni di protezione dell'orchestrator (a pagina 183).

- Proprietà

  Consultare la sezione Configurazione delle proprietà Touchpoint dell'orchestrator (a pagina 176).

- moduli

  Consultare la sezione Sostituzione delle impostazioni della categoria operatore ereditate dall'ambiente (a pagina 187).

- trigger

  Consultare la sezione Attivazione di trigger per un orchestrator (a pagina 188).

- Norme

  Consultare la sezione Configurare le norme per l'orchestrator (a pagina 189).

- Mirroring

  Consultare la sezione Configurare il mirroring di orchestrator (a pagina 192).

- Audit Trail

  Consultare la sezione Visualizzazione dell'itinerario di controllo per un orchestrator (a pagina 347).

## Visualizzazione delle impostazioni di protezione dell'orchestrator

La maggior parte delle impostazioni della scheda Protezione viene creata durante il processo di installazione dell'orchestrator di dominio. Non è possibile modificare nessuna di queste impostazioni mediante l'interfaccia utente. È possibile modificare le impostazioni reinstallando l'orchestrator di dominio.

La casella di controllo Eredita si applica solo all'Intervallo di aggiornamento della cache CA EEM (in secondi). È possibile accorciare l'intervallo di aggiornamento se si desidera che CA Process Automation riceva più velocemente le modifiche effettuate in CA EEM.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Nel riquadro Browser di configurazione, espandere Orchestrator.
3. Selezionare un orchestrator. Nella scheda Protezione, è possibile visualizzare le impostazioni di protezione.
4. Per aggiornare le impostazioni:
    a. Fare clic su Blocca.
    b. Deselezionare la casella di controllo Eredita.
    c. Aggiornare il valore Intervallo di aggiornamento della cache CA EEM.
    d. Fare clic su Salva.
    e. Fare clic su Sblocca.

**Ulteriori informazioni:**

Visualizzazione o ripristino delle impostazioni di protezione per un ambiente selezionato (a pagina 158)
Configurazione delle impostazioni di protezione di CA EEM per il dominio (a pagina 140)

## Configurazione delle proprietà di host dell'orchestrator

È possibile configurare le proprietà di host per un orchestrator selezionato e visualizzare le informazioni di sola lettura.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo Orchestrator.
3. Selezionare l'orchestrator da configurare, quindi fare clic su Blocca.

4. Fare clic sulla scheda Proprietà per visualizzare le impostazioni di proprietà dell'orchestrator di sola lettura.
   - Dominio
   - Nome host
   - Nome dell'orchestrator
   - Stato
5. Configurare i campi seguenti:

   **Ripristino automatico operatori**

   Specifica se il ripristino viene eseguito in modo automatico. Il ripristino si applica agli operatori non riusciti con SYSTEM_ERROR i cui processi recuperabili sono in stato BLOCCATO, IN ESECUZIONE o IN ATTESA al momento dell'attivazione del processo di ripristino. Se il ripristino è impostato su Automatico, ogni orchestrator nell'ambiente avvia automaticamente il ripristino non appena l'orchestrator torna a essere attivo. Il ripristino avvia l'esecuzione dei processi interessati e i relativi operatori iniziano l'esecuzione su questo orchestrator.

   **Valori:** questa proprietà presenta i valori seguenti:

   - **Eredita dall'ambiente**: utilizzare il valore configurato per questo campo nelle proprietà dell'ambiente.
   - **True**: il ripristino automatico è abilitato.
   - **False**: il ripristino automatico è disabilitato.

   **Impostazione predefinita:** Eredita dall'ambiente.

**Crea corrispondenza solo nei gruppi host?**

Specifica l'ambito di ricerca per una destinazione dell'operatore quando la voce di campo Destinazione è un indirizzo IP o un nome host (FQDN). È possibile procedere con l'esecuzione dell'operatore sulla destinazione solo quando quest'ultima è nota a CA Process Automation. Selezionare Disabilitato per avviare una ricerca più ampia. Selezionare Abilitato qui e Disabilitato nel campo successivo per una ricerca più limitata.

**Nota:** Una ricerca DNS di un nome host specificato consente di individuare gli indirizzi IP associati, mentre una ricerca DNS dell'indirizzo IP consente di individuare i nomi host associati.

**Valori:** questa proprietà presenta i valori seguenti:

- **Eredita dall'ambiente**: utilizzare il valore configurato per questo campo nelle proprietà dell'ambiente.
- **Abilitato**: l'ambito della ricerca dipende a seconda se il campo Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host? è abilitato o disabilitato.

  Se la ricerca DNS è disabilitata, viene cercato: il riferimento di gruppo host a un host remoto (esatto)

  Se la ricerca DNS è abilitata, viene cercato: il riferimento di gruppo host a un host remoto (esatto o risultato di ricerca DNS)
- **Disabilitato**: i componenti di dominio vengono cercati nell'ordine seguente:

  Touchpoint (esatto o risultato di ricerca DNS)

  Orchestrator (esatto o risultato di ricerca DNS)

  Agente (esatto o risultato di ricerca DNS)

  Touchpoint proxy con mapping su un host remoto (esatto o risultato di ricerca DNS)

  Il riferimento di gruppo host a un host remoto (esatto o risultato di ricerca DNS)

**Impostazione predefinita:** Eredita dall'ambiente.

**Eseguire la ricerca DNS durante l'impostazione della corrispondenza della destinazione nei gruppi host?**

**Nota:** Questo campo viene abilitato quando l'opzione Crea corrispondenza solo nei gruppi host è impostata su Abilitato.

Specifica se limitare la ricerca tramite i riferimenti di gruppo host al tipo di voce. Ad esempio, quando il tipo di voce del campo Destinazione è un FQDN, cercare solamente modelli di nome host. Quando il tipo di voce di campo Destinazione è un indirizzo IP, cercare solo le subnet. Quando viene inclusa una ricerca DNS, si può accettare anche un riferimento di gruppo host per l'altro tipo, come risolto da una ricerca DNS.

**Valori:** questa proprietà presenta i valori seguenti:

- **Eredita dall'ambiente**: utilizzare il valore configurato per questo campo nelle proprietà dell'ambiente.
- **Abilitato**: vengono cercati tutti i riferimenti di gruppo host. I riferimenti di gruppo host per nomi host sono modelli (espressioni regolari) che possono includere il nome host specificato. I riferimenti di gruppo host per gli indirizzi IP sono subnet di indirizzo IP espresse in notazione CIDR che possono includere l'indirizzo IP specificato. Estendere la ricerca a tutti i riferimenti di gruppo host. Eseguire la ricerca per trovare una corrispondenza esatta o una corrispondenza con il risultato di ricerca DNS.
- **Disabilitato**: si limita la ricerca ai riferimenti di gruppo host che includono una corrispondenza esatta con la voce del campo Destinazione.

**Impostazione predefinita:** Eredita dall'ambiente.

6. Fare clic su Salva.
7. Fare clic su Sblocca.

## Sostituzione delle impostazioni della categoria operatore ereditate dall'ambiente.

Le impostazioni della categoria operatore vengono configurate sulla scheda Moduli. Le impostazioni della categoria operatore che sono state configurate a livello di ambiente o ereditate dalle impostazioni configurate a livello di dominio vengono visualizzate come Eredita dall'ambiente. Un amministratore con diritti di amministratore della configurazione di ambiente può abilitare qualsiasi categoria operatore e sostituire le impostazioni ereditate a livello di orchestrator.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il riquadro Orchestrator.
3. Selezionare l'orchestrator da configurare, quindi fare clic su Blocca.
4. Fare clic sulla scheda Moduli.
5. Scegliere una categoria operatore, fare clic su Eredita da ambiente, e selezionare Abilita dall'elenco a discesa.

   **Nota:** è possibile disattivare una categoria operatore a livello di orchestrator selezionando Disabilita dall'elenco a discesa.
6. Fare clic con il pulsante destro del mouse sulla categoria operatore e selezionare Modifica.

   Le impostazioni vengono visualizzate.
7. Modificare una o più impostazioni ereditate.

   **Nota:** per ulteriori informazioni, consultare la sezione Configurazione di categorie operatore (a pagina 276).
8. Fare clic su Salva e chiudi.

   I valori configurati nella finestra di dialogo aperta vengono salvati.
9. Fare clic sul pulsante Salva nella barra degli strumenti.

   Le modifiche salvate vengono applicate alla configurazione di CA Process Automation.
10. Ripetere i passaggi 5-9 per ciascuna categoria operatore da aggiornare.
11. Selezionare l'orchestrator configurato e fare clic su Sblocca.

**Ulteriori informazioni:**

Configurazione di Utilità di rete (a pagina 306)
Configurazione di Servizi Web (a pagina 311)
Configurazione di Controllo processo (a pagina 308)
Configurazione di Gestione file (a pagina 302)
Configurazione di Esecuzione comando: Proprietà Telnet predefinite (a pagina 283)

## Attivazione di trigger per un orchestrator

Un amministratore con diritti di configurazione dell'ambiente può gestire i trigger a livello di orchestrator. Un trigger si attiva modificando il suo stato in Eredita dall'ambiente o in Abilitato e ignorando le impostazioni a livello di dominio. Per visualizzare le impostazioni correnti di un trigger, è necessario modificare lo stato in Abilitato e selezionare Modifica. Se si accettano le impostazioni, configurare il trigger impostandolo su Eredita dall'ambiente. Se non si accettano le impostazioni perché sono incomplete o non sono adatte all'orchestrator, è possibile configurare i campi e lasciare lo stato impostato su Abilitato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il riquadro Orchestrator.
3. Fare clic con il tasto destro del mouse sull'orchestrator selezionato e selezionare Blocca.
4. Fare clic sulla scheda Trigger.

   Se i trigger non sono stati configurati a livello di orchestrator, si trovano nello stato Disabilitato.

5. Fare clic con il tasto destro del mouse sul trigger che si desidera esaminare, quindi fare clic su Modifica.

   I campi visualizzano i valori che possono essere utilizzati lasciandoli invariati o modificandoli.

6. Se il trigger è completamente configurato con valori che si desidera vengano utilizzati dall'orchestrator, selezionare Eredita dall'ambiente dall'elenco a discesa Attiva/Disattiva, quindi fare clic su Chiudi.

7. Se il trigger è completamente configurato o si desidera specificare valori diversi per l'orchestrator selezionato, procedere come indicato di seguito:

   a. Selezionare Abilita dall'elenco a discesa Attiva/Disattiva.

   b. Per le descrizioni dei campi e altre informazioni attinenti ai singoli trigger, consultare Amministrazione dei trigger (a pagina 323).

   c. Se il trigger selezionato è il trigger di posta e l'orchestrator non è l'orchestrator di dominio, fare clic su Sfoglia e selezionare il file di processo predefinito.

      Il campo del processo di attivazione predefinito viene popolato con il percorso corretto per questo orchestrator.

   d. Fare clic su Chiudi.

8. Fare clic su Salva.

9. Fare clic con il tasto destro del mouse sull'orchestrator bloccato e fare clic su Sblocca.

**Ulteriori informazioni:**

Configurazione delle proprietà di trigger di file a livello di dominio (a pagina 329)
Configurazione delle proprietà di trigger di SNMP a livello di dominio (a pagina 334)
Amministrazione di trigger (a pagina 323)
Configurazione delle proprietà di trigger di posta a livello di dominio (a pagina 330)

## Configurazione delle policy Orchestrator

Le impostazioni delle policy orchestrator specificano le impostazioni di cronologia relative ai processi eseguiti sull'orchestrator. Specificano, inoltre, la pianificazione predefinita e il processo predefinito nella libreria. È possibile configurare policy distinte per orchestrator diversi.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.

2. Dal Browser di configurazione, selezionare l'orchestrator da configurare, quindi fare clic su Blocca.

3. Fare clic sulla scheda Policy.
4. Selezionare se consentire agli utenti di salvare un oggetto modificato come la stessa versione in fase di archiviazione o se automatizzare il controllo di versione dell'oggetto creando una nuova versione in fase di archiviazione.
5. Se è stato definito un processo che specifica i gestori di processo predefiniti con regole per la modifica di corsia e la gestione delle eccezioni, individuare tale processo e selezionarlo.
6. Specificare i requisiti per conservare le istanze dei processi che sono stati eseguiti.
   a. Selezionare il numero minimo di giorni di conservazione delle istanze di processo eseguite su un touchpoint o un host remoto. Se si configura un giorno, il processo resta nella libreria per almeno 24 ore prima di essere archiviato.
   b. Selezionare il numero minimo di istanze di processo non riuscite da conservare nella cronologia.
   c. Selezionare il numero minimo di istanze completate per l'oggetto di processo da conservare nella cronologia.
   d. Selezionare il numero massimo di messaggi di log che è possibile visualizzare quando l'istanza di processo viene aperta da una Visualizzazione processo.
7. Selezionare il numero minimo di giorni per l'archiviazione di un allegato nel database di CA Process Automation prima di eliminarlo.

   Gli utenti possono utilizzare i servizi Web per attivare i processi. Un utente può avviare direttamente un processo o pianificare un Modulo di richiesta di avvio. Gli utenti possono inviare i file come allegati nelle chiamate dei servizi Web. Quando una chiamata di servizio Web attiva un processo, gli utenti possono accedere ai file all'interno di quel processo. Un utente può utilizzare l'operatore SOAP per inoltrare un allegato alla chiamata di servizi Web in uscita.

8. Specificare i requisiti per le istanze del processo di eliminazione definitiva che sono state eseguite sull'orchestrator selezionato e successivamente archiviate. In alternativa, eliminare su richiesta in modo definitivo le istanze del processo avviate entro un intervallo di date specificato.

   a. Definisce la policy per l'eliminazione definitiva dei dati archiviati. Le opzioni consentono di:

      **Non eliminare i dati archiviati**

      Le istanze di processo archiviate vengono conservate fino all'eliminazione manuale.

      **Elimina dati archiviati ogni giorno**

      Le istanze di processo archiviate vengono eliminate come attività pianificata in base alle impostazioni dei due campi seguenti.

      **Elimina dati senza eseguire l'archiviazione**

      Le istanze di processo vengono conservate come attive per un intervallo configurato. Trascorso tale intervallo, i dati vengono eliminati. Nessuna istanza di processo viene archiviata.

   b. Definire l'ora del giorno (nel formato hh:mm) in cui eliminare le istanze archiviate e conservate per il numero configurato di giorni.

   c. Definire il numero di giorni per conservare le istanze di processo archiviate. Una volta conservata per il numero di giorni configurato, l'istanza archiviata viene eliminata all'ora indicata.

   d. Per eliminare in modo definitivo le istanze archiviate che sono state avviate entro un intervallo di tempo specificato dall'orchestrator corrente, fare clic sul pulsante Elimina istanza archiviata, selezionare un intervallo di date e fare clic su OK.

9. Specificare se richiedere l'autenticazione quando un utente tenta di accedere ad allegati esterni a CA Process Automation. Se l'opzione è selezionata, gli utenti devono fornire credenziali valide per accedere agli allegati.

10. Specificare se applicare la protezione runtime. Se selezionata, la Protezione runtime viene abilitata per i processi impostati su Abilita o che ereditano un'impostazione abilitata.

    **Nota:** Se si selezionano le opzioni Abilita la protezione runtime ed Esegui come titolare come opzione di protezione runtime per un processo, utilizzare l'opzione Imposta titolare per stabilire la titolarità di ciascun oggetto di processo interessato. Per ulteriori informazioni, consultare la guida in linea o la *Guida alla progettazione dei contenuti*.

11. Fare clic su Salva.

12. Fare clic su Sblocca.

## Configurazione del mirroring di orchestrator

Gli orchestrator eseguono il mirroring di dati e informazioni di configurazione memorizzati nell'orchestrator di dominio. L'impostazione di mirroring specifica la frequenza dei controlli di un orchestrator per eventuali modifiche sull'orchestrator di dominio. Le modifiche all'orchestrator di dominio vengono applicate all'orchestrator sull'host locale. È possibile impostare l'intervallo di mirroring per un orchestrator.

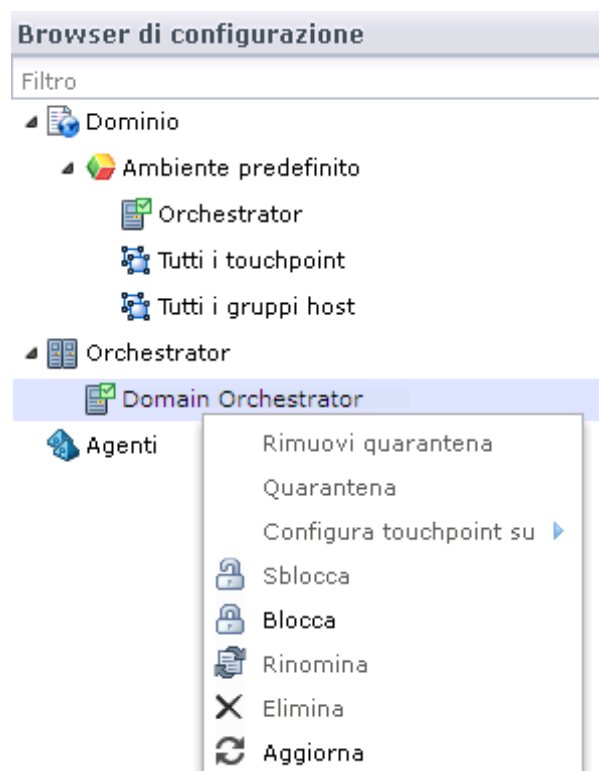
Quando si seleziona un orchestrator in cluster, l'intervallo impostato è valido per il mirroring in tutti i nodi attivi nel cluster. Un nodo cluster può essere non attivo quando gli altri nodi nel cluster vengono aggiornati. In questo caso, il mirroring per il nodo non attivo avviene all'avvio.

**Nota:** È possibile caricare un file JAR nella cartella Risorse orchestrator dell'Orchestrator di dominio. Quando si riavvia l'orchestrator di dominio, CA Process Automation effettua la distribuzione del file all'orchestrator di dominio. L'orchestrator di dominio esegue la duplicazione del file all'intervallo di mirroring configurato, dopo il quale verranno riavviati gli altri orchestrator. Quando gli orchestrator vengono riavviati, il file duplicato può essere utilizzato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Nel riquadro Browser di configurazione, espandere Orchestrator.
3. Selezionare l'orchestrator da configurare, quindi fare clic su Blocca.
4. Fare clic sulla scheda Mirroring.
5. Nel campo Intervallo di mirroring (minuti), selezionare l'intervallo tra le volte in cui l'orchestrator selezionato richiede gli aggiornamenti dall'orchestrator di dominio. Il prodotto esegue il mirroring di qualsiasi modifica apportata all'orchestrator selezionato nell'intervallo specificato.
6. Fare clic su Salva.
7. Nel riquadro Browser di configurazione, selezionare l'orchestrator configurato e fare clic su Sblocca.

# Gestione dell'host dell'orchestrator

Quando si seleziona un orchestrator nel nodo Orchestrator, le informazioni visualizzate sono relative all'host, invece che al touchpoint.

Consultare gli argomenti seguenti associati alle opzioni di menu per l'host dell'orchestrator.

- Rimuovi quarantena

  Consultare la sezione Rimozione di un orchestrator dalla quarantena (a pagina 195).

- Quarantena

  Consultare la sezione Messa in quarantena di un orchestrator (a pagina 194).

- Configura touchpoint su

  Consultare la sezione Configurazione delle proprietà Touchpoint dell'orchestrator (a pagina 176).

- Sblocca - selezionare l'orchestrator e fare clic su Sblocca.
- Blocca - selezionare l'orchestrator e fare clic su Blocca.
- Rinomina - selezionare l'orchestrator e digitare un nuovo nome.
- Elimina - selezionare l'orchestrator e fare clic su Elimina. Non è possibile eliminare l'orchestrator di dominio.
- Aggiorna - selezionare l'orchestrator e fare clic su Aggiorna.

## Messa in quarantena di un orchestrator

È possibile mettere in quarantena qualsiasi orchestrator, ad eccezione dell'orchestrator di dominio. La quarantena isola un orchestrator. Non è possibile eseguire gli operatori su un orchestrator in quarantena. Non è possibile aprire la libreria di un orchestrator in quarantena. Non è pertanto possibile creare o salvare oggetti di libreria su un orchestrator in quarantena.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il tasto destro del mouse sul dominio e selezionare Blocca.
3. Fare clic con il pulsante destro del mouse sull'ambiente contenente l'orchestrator che si desidera mettere in quarantena e selezionare Blocca.
4. Espandere il nodo Orchestrator.
5. Fare clic con il tasto destro del mouse sull'orchestrator che si desidera mettere in quarantena, quindi fare clic su Blocca.
6. Fare di nuovo clic con il pulsante destro del mouse sull'orchestrator, quindi selezionare Quarantena.

7. Fare clic su Salva.
8. Fare clic con il tasto destro del mouse sull'orchestrator e selezionare Sblocca.
9. Fare clic con il pulsante destro del mouse sull'ambiente bloccato, quindi selezionare Sblocca.
10. Fare clic con il tasto destro del mouse su Dominio e selezionare Sblocca.

**Ulteriori informazioni:**

Rimozione di un orchestrator dalla quarantena (a pagina 195)
Eliminazione di un touchpoint dell'orchestrator (a pagina 169)
Disabilitazione di un touchpoint di orchestrator (a pagina 181)

## Rimozione di un orchestrator dalla quarantena

Se la quarantena è stata creata per motivi diversi dalla rimozione dell'orchestrator, rimuovere l'orchestrator dalla quarantena se le condizioni necessarie non esistono più.

**Per rimuovere un orchestrator dalla quarantena**

1. Fare clic sulla scheda Configurazione.
2. Espandere il riquadro Orchestrator.
3. Fare clic con il pulsante destro del mouse sull'orchestrator di destinazione messo in quarantena, quindi fare clic su Blocca.
4. Fare di nuovo clic con il tasto destro sull'orchestrator, quindi fare clic su Rimuovi dalla quarantena.
5. Fare clic con il tasto destro del mouse sull'orchestrator e selezionare Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che chiede se si desidera salvare le modifiche.
6. Fare clic su Sì.

## Interruzione dell'orchestrator

Solo gli amministratori con credenziali di amministratore sul server in cui è installato l'orchestrator possono interromperlo.

**Importante.** In caso di arresto anomalo di un orchestrator, la cartella temporanea seguente può sviluppare file di grandi dimensioni. Se si verifica questo evento, è possibile eliminare la cartella tmp in modo sicuro:

`install_dir/server/c2o/tmp`

**Attenersi alla procedura seguente:**

1. Utilizzando le credenziali di amministratore, accedere all'host in cui è installato l'orchestrator di destinazione.
2. In caso di accesso a un host di Windows, è possibile interrompere il servizio Orchestrator dal menu Start, dalla finestra Servizi o dalla riga di comando. Completare una delle azioni seguenti:
   - Nel menu Start, selezionare Programmi, CA, CA Process Automation 4.0, quindi Arresta servizio dell'orchestrator.
   - Selezionare Strumenti di amministrazione e Servizi da Pannello di controllo. Selezionare il servizio seguente e fare clic su Arresta:

     ```
     Orchestrator CA Process Automation (C:/Program
     Files/CA/PAM/server/c2o)
     ```
   - Aprire un prompt dei comandi ed eseguire lo script riportato:

     `install_dir/server/c2o/bin/stopc2osvc.bat`
3. In caso di accesso a un host UNIX o Linux, completare i passaggi seguenti:

   a. Modificare le directory in ${PAM_HOME}/server/c2o/. Ad esempio, modificare le directory in:

   ```
   /usr/local/CA/PAM/server/c2o
   ```

   b. Eseguire lo script c2osvrd.sh con l'opzione di arresto. Ad esempio:

   ```
   ./c2osvrd.sh stop
   ```

## Avvio dell'orchestrator

Solo gli amministratori con credenziali di amministratore sul server in cui è installato l'orchestrator possono riavviarlo.

**Attenersi alla procedura seguente:**

1. Utilizzando le credenziali di amministratore, accedere all'host in cui è installato l'orchestrator di destinazione.
2. In caso di accesso a un host di Windows, è possibile riavviare il servizio Orchestrator dal menu Start, dalla finestra Servizi o dalla riga di comando. Eseguire una delle attività seguenti:
   - Selezionare Programmi, CA, CA Process Automation, quindi Avvia servizio dell'orchestrator dal menu Start.
   - Selezionare Strumenti di amministrazione e Servizi da Pannello di controllo. Selezionare il servizio seguente e fare clic su Avvia:

     `Orchestrator CA Process Automation (C:/Program Files/CA/PAM/server/c2o)`
   - Aprire un prompt dei comandi ed eseguire lo script riportato:

     *install_dir*`/server/c2o/bin/startc2osvc.bat`
3. In caso di accesso a un host UNIX o Linux, eseguire le attività seguenti:
   a. Modificare le directory in ${PAM_HOME}/server/c2o/. Ad esempio, modificare le directory in:

      `/usr/local/CA/PAM/server/c2o`

   b. Eseguire lo script c2osvrd.sh con l'opzione di avvio. Ovvero, eseguire:

      `./c2osvrd.sh start`

**Nota:** dopo avere avviato il servizio per l'orchestrator di dominio, avviare CA Process Automation.

**Ulteriori informazioni:**

Configurazione delle proprietà di trigger di file a livello di dominio (a pagina 329)
Configurazione delle proprietà di trigger di SNMP a livello di dominio (a pagina 334)
Amministrazione di trigger (a pagina 323)
Configurazione delle proprietà di trigger di posta a livello di dominio (a pagina 330)

## Eliminazione definitiva delle istanze di processo archiviate da un orchestrator

È possibile eliminare su richiesta le istanze di processo eseguite durante l'intervallo di date indicato.

Eliminare le istanze di processo archiviate dal database di runtime di un orchestrator nelle situazioni seguenti:

- Spazio insufficiente: il numero elevato di istanze archiviate causa un rallentamento delle prestazioni.
- La policy Orchestrator è impostata in modo da disattivare l'eliminazione automatica.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione ed espandere il nodo Orchestrator nel browser di configurazione.

   Il nodo espanso mostra tutti gli orchestrator nel dominio.

2. Fare clic con il pulsante destro del mouse sull'orchestrator con le istanze di processo archiviate da eliminare, quindi fare clic su Blocca.
3. Fare clic sulla scheda Policy.
4. Fare clic sul pulsante Elimina istanza archiviata nella parte inferiore del riquadro.
5. Nella finestra di dialogo Elimina istanza archiviata, definire l'intervallo di date in cui eliminare le istanze archiviate.
   a. Fare clic sul pulsante di calendario Data di inizio e selezionare Oggi o una data di inizio precedente alla data corrente.
   b. Fare clic sul pulsante di calendario Data di fine e selezionare Oggi o una data di fine successiva a quella corrente.
   c. Fare clic su OK.
6. Fare clic su Sì nel messaggio di conferma.

   Il processo di eliminazione elimina tutte le istanze archiviate eseguite nell'intervallo di date indicato.

7. Fare clic con il tasto destro del mouse sull'orchestrator e fare clic su Sblocca.

# Capitolo 8: L'amministrazione degli agenti

Un agente è un componente che viene installato su più host in ogni ambiente. Dopo l'installazione di un agente su un host, si configura un touchpoint (entità logica) che associa l'ambiente attuale all'host agente.

Gli agenti supportano l'esecuzione dei processi. I processi sono costituiti da operatori. La maggior parte degli operatori viene eseguita sull'orchestrator. Quando l'esecuzione di un operatore avviene su un host agente, è svolta sotto il controllo dell'orchestrator, cui vengono restituiti i risultati. L'orchestrator esegue il processo principale.

Per garantire che un host agente sia sempre disponibile per l'elaborazione, associare più host agente a un singolo touchpoint. Un touchpoint associa uno o più agenti a un ambiente specificato. I responsabili di progettazione dei contenuti, in genere, utilizzano come destinazione un host agente impostando come tale anche il relativo touchpoint.

Per eseguire gli operatori su host remoti privi di agenti, associare un agente a touchpoint proxy o gruppi host. È possibile eseguire gli operatori su un host remoto senza agenti quando è configurata una connessione SSH dall'host agente sull'host remoto di destinazione. Per l'esecuzione su un host remoto, gli operatori utilizzano come destinazione il touchpoint proxy.

Per informazioni sulla configurazione del failover (impostazioni di priorità) o del bilanciamento del carico tra agenti associati allo stesso touchpoint, consultare la sezione Amministrazione dei touchpoint (a pagina 223).

Per informazioni sulla creazione di connessioni SSH, consultare le sezioni Amministrazione dei touchpoint proxy (a pagina 245) e Amministrazione di gruppi host (a pagina 253).

Questa sezione contiene i seguenti argomenti:

# Configurazione di agenti per il supporto delle destinazioni dell'operatore

La configurazione di agenti in un ambiente di progettazione in genere si limita alla configurazione di un piccolo insieme di touchpoint, ognuno mappato su un agente singolo. Se il numero di host disponibili è ridotto, è possibile associare più touchpoint allo stesso agente.

Le configurazioni di agenti più solide sono tipiche negli ambienti di produzione. Di seguito si riporta una descrizione delle sei opzioni disponibili e una tabella riassuntiva di riferimento. Utilizzare queste informazioni per pianificare e implementare la configurazione degli agenti nell'ambiente di produzione.

**Esecuzione dell'operatore su un host agente specifico.**

Questa opzione è la più facile da implementare durante l'esecuzione di un operatore su un host con un agente. Questa opzione è accettabile in un ambiente di sviluppo o di test.

**Destinazione effettiva**

Nome host o indirizzo IP della destinazione.

**Requisito di installazione**

Installare un agente sull'host di destinazione.

**Requisito di associazione**

Definizione di un touchpoint per l'associazione di un agente all'ambiente di produzione.

**Destinazione dell'operatore**

Immettere il nome del touchpoint. In alternativa, è possibile immettere l'ID dell'agente.

**Esecuzione dell'operatore sull'agente con la priorità più elevata, tra i diversi agenti possibili.**

Questa opzione consente di specificare che l'operatore sia eseguito sull'host preferito se disponibile, altrimenti sul successivo host in ordine di preferenza. L'utente definisce i criteri che rendono un host preferito rispetto a un altro. È possibile configurare un touchpoint per impostare l'esecuzione di un operatore specifico sempre sull'host con capacità maggiore. Oppure è possibile riservare tali host ed utilizzarli per l'esecuzione solo nel caso in cui tutti gli altri candidati siano occupati.

**Destinazione effettiva**

Sconosciuta. Registrare i nomi host degli host di destinazione candidati, secondo l'ordine di preferenza.

**Requisito di installazione**

Installare un agente su ogni host di destinazione candidato.

**Requisito di associazione**

Definire un touchpoint e associarlo a ciascuno degli host di destinazione candidati. Nella definizione di touchpoint, specificare il grado di priorità per ciascuno.

**Destinazione dell'operatore**

Immettere il nome del touchpoint.

**Esecuzione dell'operatore sull'agente meno occupato, tra i diversi agenti possibili.**

Questa opzione richiede più tempo di implementazione rispetto a un touchpoint associato a un agente, ma è un'opzione solida quando si utilizza come destinazione un host con un agente. Questa opzione viene progettata per un ambiente di produzione in cui è importante che il processo sia eseguito all'ora pianificata.

**Destinazione effettiva**

Sconosciuta. Registrare i nomi host degli host di destinazione candidati.

**Requisito di installazione**

Installare un agente su ogni host di destinazione candidato.

**Requisito di associazione**

Definire un touchpoint e associarlo a ciascuno degli host di destinazione candidati. Nella definizione di touchpoint, immettere lo stesso numero di priorità per ciascuna associazione. Questa implementazione consente di ottenere il bilanciamento del carico.

**Destinazione dell'operatore**

Immettere il nome del touchpoint.

**Esecuzione simultanea dell'operatore su più host agente.**

L'uso del gruppo touchpoint consente di eseguire contemporaneamente un operatore su tutti gli host associati ai touchpoint nel gruppo.

**Destinazioni effettive**

Registrare il nome host di ciascun host di destinazione.

**Requisito di installazione**

Installare un agente su ogni host di destinazione.

**Requisito di associazione**

- Definire un touchpoint separato per ciascuno di questi agenti.
- Definire un gruppo touchpoint composto da questi touchpoint.

**Destinazione dell'operatore**

Immettere il nome del gruppo touchpoint.

**Esecuzione dell'operatore su un host remoto specifico.**

A volte non è possibile installare un agente su un host che si desidera utilizzare come destinazione per un operatore. In tal caso, definire un agente come touchpoint proxy. Creare una connessione SSH dall'host con l'agente all'host remoto di destinazione.

**Destinazione effettiva**

Registrare il nome host o l'indirizzo IP dell'host remoto che è la destinazione.

**Abilitazione dell'host di origine**

Registrare il nome host dell'host di origine che può connettersi alla destinazione con una connessione SSH.

**Requisito di connettività**

Creare la connessione SSH dall'host di origine all'host remoto.

**Requisito di installazione**

Installare un agente sull'host di origine.

**Requisito di associazione**

Definire un touchpoint proxy sull'host di origine e specificare i dettagli di connessione all'host di destinazione remoto.

**Destinazione dell'operatore**

Immettere il nome di touchpoint proxy.

**Esecuzione dell'operatore su un host remoto, in cui la destinazione può cambiare a ogni esecuzione.**

Questa opzione consente di definire l'host remoto di destinazione prima del runtime, quando si specifica la destinazione con il relativo nome host o indirizzo IP. La destinazione deve appartenere a un gruppo host. Un gruppo host è un gruppo con un modello di nome host o di indirizzo IP comune. Gli host con un modello di indirizzo IP comune appartengono alla stessa subnet.

**Destinazione effettiva**

Sconosciuta. Registrare i nomi host degli host di destinazione remoti candidati.

**Abilitazione dell'host di origine**

Registrare il nome host dell'host di origine che può connettersi a ciascuna delle destinazioni candidate con una connessione SSH.

**Requisito di connettività**

Creare la connessione SSH dall'host di origine a ciascun host remoto.

**Requisito di installazione**

Installare un agente sull'host di origine.

**Requisito di associazione**

Definire un gruppo host sull'host di origine con un modello comune agli host remoti.

**Destinazione dell'operatore**

Immettere il nome host o l'indirizzo IP dell'host remoto di destinazione. Esprimere la destinazione dell'operatore in un set di dati. È possibile modificare i set di dati, anche quando sono importati con un processo non modificabile.

Utilizzare la tabella seguente come guida per la creazione di tabelle di riepilogo. La documentazione sotto forma di tabelle di riepilogo può servire ad altri utenti per trovare queste informazioni quando l'utente corrente non è disponibile.

| Tipo di destinazione | Associazione di agente | Altra configurazione | Destinazione dell'operatore |
|---|---|---|---|
| Un host singolo | Un nuovo touchpoint | N/D | Nome touchpoint |
| Uno tra più host, in ordine di priorità | Un touchpoint esistente | Specificare la priorità in cui selezionare l'host di destinazione. | Nome touchpoint |
| Uno tra più host (nessuna priorità) | Un touchpoint esistente | Assegnare la stessa priorità a ciascun host di destinazione candidato. | Nome touchpoint |
| Più host contemporaneamente | Un nuovo touchpoint | Creare un gruppo touchpoint con tutti i touchpoint. | Nome gruppo touchpoint |

| Tipo di destinazione | Associazione di agente | Altra configurazione | Destinazione dell'operatore |
|---|---|---|---|
| Un host remoto singolo | Un touchpoint proxy | Creare la connessione SSH dall'host agente all'host remoto di destinazione. | Nome di touchpoint proxy |
| Uno tra più host remoti | Un gruppo host | Creare la connessione SSH dall'host agente a ciascun host remoto di destinazione. | Nome host o indirizzo IP di destinazione |

**Ulteriori informazioni**

Informazioni sulla comunicazione degli agenti (a pagina 221)

# Installazione interattiva di un agente

I processi possono includere operatori che devono essere eseguiti su server con un'applicazione di destinazione, database o sistema. Se possibile, installare un agente su un server di questo tipo. Se non è possibile, installare l'agente su un host che può essere connesso con tale server attraverso SSH.

**Importante.** Prima di installare un agente, verificare che l'orchestrator di dominio sia in esecuzione.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic sul riquadro Installazione.
3. Fare clic su Installa per Installa agente.

   Viene visualizzata una finestra di dialogo che mostra l'avanzamento per il download dell'applicazione.
4. Se si riceve un avviso di protezione, fare clic su Esegui.

   Viene visualizzata la finestra di dialogo per la selezione della lingua. La lingua del computer host è selezionata per impostazione predefinita.
5. Fare clic su OK o selezionare un'altra lingua e fare clic su OK.

   Viene visualizzata la pagina introduttiva per la procedura guidata di installazione agente di CA Process Automation.
6. Fare clic su Avanti.

   Viene visualizzato il contratto di licenza.

7. Leggere la licenza. Se si accettano i termini, fare clic su Accetto i termini del contratto di licenza. Fare clic su Avanti.

   Viene visualizzata la pagina per l'impostazione della directory principale di Java.

8. Se la directory principale di Java visualizzata non è corretta, sfogliare la cartella JRE.

   Tutte le piattaforme supportano jre6. Windows supporta jre6 e jre7.

   Fare riferimento al percorso di esempio seguente per la piattaforma Windows:

   ```
   C:\Program Files\Java\jdk1.7.0_45
   ```

9. Fare clic su Avanti.

   Viene visualizzata la pagina per selezionare la directory di destinazione. In un host Windows, segue il percorso predefinito:

   ```
   C:\Program Files\CA\Agente PAM
   ```

10. Fare clic su Avanti per accettare l'impostazione predefinita, oppure immettere una directory di destinazione per il nuovo agente, quindi fare clic su Avanti.

    Viene visualizzata la pagina per selezionare una cartella Menu Start.

11. (Solo Windows) Fare clic su Avanti per accettare Agente CA Process Automation come collegamento al Menu Start, oppure immettere un nuovo nome e fare clic su Avanti.

    - (Facoltativo) Creare collegamenti per tutti gli utenti su questo host.
    - (Facoltativo) Non creare una cartella nel menu Start.

12. Esaminare l'URL di dominio. Questo è l'URL da cui è stata avviata l'installazione dell'agente. Fare clic su Avanti.

13. Se il dominio è protetto, inserire una password.

14. Completare la pagina Proprietà generali, quindi fare clic su Avanti.

    a. Immettere il nome dell'host agente per Host agente. Questo nome identifica l'host da cui è stata avviata l'installazione.

    b. Modificare o accettare il nome visualizzato predefinito dell'host.

    c. Se l'installazione dell'agente è stata avviata da un host di Windows, selezionare Installa come servizio Windows.

    d. Per forzare una nuova connessione per ciascuna comunicazione da un orchestrator a un agente, selezionare Usa comunicazione non più in uso.

       Si consiglia di lasciare *deselezionata* questa casella di controllo. Il valore predefinito Comunicazioni semplificate viene preferito perché utilizza una connessione persistente.

    e. Se si seleziona Usa comunicazione non più in uso, accettare 7003 come Porta agente a meno che tale porta non sia già in uso. Se si utilizza la porta predefinita, immettere il numero di una porta non utilizzata, ad esempio 57003, come porta in cui l'agente rileva la comunicazione con gli orchestrator.

       **Nota:** Se non si utilizza la comunicazione non più in uso, gli orchestrator utilizzano una connessione con socket Web (stabilita dagli agenti) per comunicare con gli agenti. Gli orchestrator utilizzano la porta 80 per comunicare con gli agenti tramite HTTP. Gli orchestrator utilizzano la porta 443 per comunicare con gli agenti tramite HTTPS.

    f. Selezionare Avvia agente al completamento dell'installazione.

       L'avvio dell'agente consente di visualizzare l'agente attivo e di continuare con la configurazione.

15. Fare clic su Avanti per accettare la directory temporanea predefinita per l'esecuzione degli script oppure immettere un altro percorso e fare clic su Avanti.

    **Nota:** il percorso non può contenere spazi.

    Viene visualizzata la pagina Imposta policy di esecuzione PowerShell.

16. Completare l'impostazione in uno dei modi seguenti.

    - Per eseguire gli script di Windows PowerShell attraverso questo agente:

      a. Selezionare la casella di controllo Imposta policy di esecuzione PowerShell.

      b. Accedere alla posizione dell'host di PowerShell se è diversa dal valore predefinito visualizzato.

      c. Fare clic su Avanti.

    - Se non si utilizza Windows PowerShell, fare clic su Avanti.

    L'installazione dell'agente si avvia.

17. Fare clic su Fine.

18. (Solo Windows) Avviare il servizio dell'agente. Fare clic su Start, Programmi, CA, Agente CA Process Automation, Avvia servizio dell'agente.
19. Fare clic sul riquadro Browser di configurazione nella scheda Configurazione.
20. Fare clic su Aggiorna. (Oppure disconnettersi ed effettuare di nuovo l'accesso.)
21. Espandere Agenti e verificare che il nome dell'agente sia incluso nell'elenco.

    **Nota:** Per utilizzare l'host agente come destinazione, configurare un touchpoint. Per utilizzare l'host agente come gateway per un host remoto, configurare un touchpoint proxy.

# Aggiunta di un touchpoint agente

Quando si installa un agente su un host, il nome visualizzato dell'agente viene visualizzato sotto al nodo Agenti. Affinché un operatore sia in grado di utilizzare tale host come destinazione, configurare un touchpoint che faccia riferimento all'host.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo Agenti.
3. Fare clic con il pulsante destro del mouse sull'agente e selezionare Configura touchpoint su, quindi selezionare l'*ambiente*.

    Viene visualizzato un messaggio che chiede se si desidera bloccare l'ambiente selezionato.
4. Fare clic su Sì per bloccare l'ambiente selezionato.

    Viene visualizzata la finestra di dialogo Aggiungi touchpoint agente.
5. Immettere un nome per il nuovo touchpoint diverso dal nome host, quindi fare clic su OK.

    Il nuovo touchpoint viene visualizzato nel nodo Tutti i touchpoint per l'ambiente associato.
6. Fare clic su Salva.
7. Selezionare l'ambiente bloccato e fare clic su Sblocca.

**Ulteriori informazioni:**

Amministrazione dei touchpoint (a pagina 223)
Amministrazione dei touchpoint proxy (a pagina 245)

# Aggiunta di un gruppo host agente

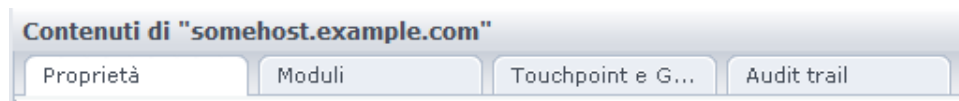
Se un operatore deve utilizzare direttamente come destinazione gli host remoti (con un indirizzo IP o un nome host), è possibile:

1. Creare un gruppo host (a pagina 256).
2. Configurare le proprietà del gruppo host (a pagina 257). È possibile aggiungere host remoti specifici o immettere modelli che includono gli host che si desidera utilizzare come destinazione.
3. Creazione delle credenziali SSH su host in un gruppo host (a pagina 262). Creare un account utente su ciascun host remoto con le credenziali immesse nelle proprietà del gruppo host.

**Ulteriori informazioni:**

Amministrazione di gruppi host (a pagina 253)

# Configurazione dei contenuti di un agente selezionato

Molte impostazioni relative alle proprietà vengono recuperate durante l'installazione dell'agente. I touchpoint associati rappresentano dettagli di configurazione univoci per gli agenti e non vengono ereditati. Le impostazioni per l'operatore sulla scheda Moduli vengono ereditate per impostazione predefinita. Le impostazioni configurate per un agente sono diverse da quelle configurate per il touchpoint dell'agente.

Il menu Agente comprende le schede seguenti:

**Proprietà**

Consultare la sezione Configurazione di proprietà dell'agente (a pagina 209).

**moduli**

Consultare la sezione Personalizzazione delle impostazioni di agente per categorie operatore (a pagina 210).

**Touchpoint e Gruppi host associati**

Consultare la sezione Visualizzazione dei touchpoint e dei gruppi host per un agente selezionato (a pagina 212).

**Audit Trail**

Consultare la sezione Visualizzazione dell'audit trail per un agente (a pagina 348).

## Configurazione di proprietà dell'agente

È possibile impostare i valori per le seguenti proprietà dell'agente:

- La frequenza con cui l'agente invia un heartbeat all'orchestrator di dominio.
- La frequenza con cui l'agente verifica la presenza di aggiornamenti per l'orchestrator di dominio.

L'agente invia un heartbeat all'avvio e in conformità alla pianificazione configurata mentre l'agente è attivo. L'orchestrator di dominio riconosce l'heartbeat o gli aggiornamenti di dominio, se disponibili. L'orchestrator di dominio invia gli aggiornamenti di mirroring all'agente in base agli intervalli di mirroring specificati.

È possibile impostare le proprietà dell'agente nel browser di configurazione.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione ed espandere Agenti nel riquadro Browser di configurazione.
2. Selezionare l'agente da configurare e fare clic su Blocca.
3. Selezionare la scheda Proprietà per l'agente selezionato.
4. (Facoltativo) Rivedere le proprietà di sola lettura seguenti:
   - Stato: attivo o non attivo
   - Nome agente: nome configurato come nome visualizzato durante l'installazione.
   - Nome host: nome configurato come host agente durante l'installazione.
   - Indirizzo host
5. (Facoltativo) Aggiornare le proprietà seguenti:
   - Intervallo di mirroring (minuti)
   - Intervallo di heartbeat (minuti): il valore predefinito a livello di dominio è 2.
   - Usa comunicazione non più in uso
6. Selezionare l'agente e fare clic su Sblocca.
7. Fare clic Sì nella finestra di dialogo Dati non salvati per salvare le modifiche.

## Personalizzazione della categoria operatore per un agente selezionato

Ogni ambiente, orchestrator e agente eredita le impostazioni configurate nella scheda Moduli per il dominio. Gli amministratori possono modificare la configurazione ai livelli inferiori della gerarchia di dominio. Gli amministratori possono abilitare categorie di operatori su qualsiasi agente e modificare le configurazioni come necessario.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere gli agenti, fare clic con il pulsante destro del mouse sull'agente da personalizzare, quindi selezionare Blocca.
3. Fare clic sulla scheda Moduli.
4. Selezionare Abilitato dall'elenco a discesa Abilita/Disabilita per la categoria di operatori da modificare.
5. Fare clic con il pulsante destro del mouse sulla stessa categoria, quindi selezionare Modifica.
6. Modificare le impostazioni di proprietà della categoria selezionata per l'agente selezionato. Per ulteriori informazioni, consultare le seguenti descrizioni di campo a livello di dominio:
   - Configurazione di Catalyst (a pagina 277).
   - Configurazione di Esecuzione comando (a pagina 283).
   - Configurazione di Database: Proprietà Oracle (a pagina 291).
   - Configurazione di Database: Proprietà del server MSSQL (a pagina 293).
   - Configurazione di Database: Proprietà MySQL (a pagina 295).
   - Configurazione di Database: Proprietà Sybase (a pagina 295).
   - Configurazione di Servizi directory (a pagina 297).
   - Configurazione di Posta elettronica (a pagina 300).
   - Configurazione di Gestione file (a pagina 302).
   - Configurazione di Trasferimento file (a pagina 304).
   - Configurazione di Utilità di rete (a pagina 306).
   - Configurazione di Controllo processo (a pagina 308).
   - Configurazione di Utilità (a pagina 309).
   - Configurazione di Servizi Web (a pagina 311).
7. Fare clic su Salva, quindi su OK nel messaggio di verifica.
8. Fare clic con il pulsante destro del mouse sull'agente bloccato, quindi selezionare Sblocca.

## Disabilitare una categoria operatore su un agente selezionato

Dalla scheda Moduli di un agente selezionato, è possibile disabilitare una o più categorie dell'operatore per tale agente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione ed espandere Agenti nel riquadro Browser di configurazione.
2. Selezionare l'agente da configurare e fare clic su Blocca.
3. Fare clic sulla scheda Moduli.
4. Selezionare una categoria dell'operatore in cui Abilita/Disabilita è impostato su Abilita o Eredita dall'ambiente.
5. Selezionare Disabilita dall'elenco a discesa Abilita/Disabilita.
6. Fare clic su Salva.
7. Fare clic su Sblocca.

   Il prodotto disabilita la categoria dell'operatore selezionata nell'agente selezionato.

**Ulteriori informazioni:**

Abilitazione o disabilitazione di una categoria operatore (a pagina 316)
Categorie operatore e dove gli operatori vengono eseguiti (a pagina 321)
Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione di Utilità di rete (a pagina 306)
Configurazione di Servizi Web (a pagina 311)
Configurazione di Gestione file (a pagina 302)
Configurazione di Esecuzione comando: Proprietà Telnet predefinite (a pagina 283)

## Configurazione di un touchpoint selezionato o di un gruppo host

Un touchpoint è un'associazione tra un agente (o orchestrator) e un ambiente. Un touchpoint proxy è un'associazione tra un agente, un host remoto e un ambiente. Un gruppo host è un'associazione tra un agente, un gruppo di host remoti e un ambiente.

Quando si aggiunge un touchpoint o un touchpoint proxy a un agente, il touchpoint viene visualizzato in Tutti i touchpoint.

Quando si aggiunge un gruppo host a un agente, il nome del gruppo host viene visualizzato in Tutti i gruppi host.

Consultare gli argomenti seguenti per informazioni sulla configurazione:

- Amministrazione dei touchpoint.
- Amministrazione dei touchpoint proxy.
- Amministrazione di gruppi host.

## Visualizzazione dei touchpoint e dei gruppi host per un agente selezionato

È possibile visualizzare i touchpoint e i gruppi host per un agente selezionato nella scheda Associated Touchpoint (Touchpoint associato).

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione ed espandere Agenti nel riquadro Browser di configurazione.
2. Selezionare l'agente di cui visualizzare i touchpoint e i gruppi host.
3. Fare clic sulla scheda Associated Touchpoint (Touchpoint associato).

   Vengono visualizzati i nomi dei touchpoint o dei gruppi host e la gerarchia (dove Dominio è il nodo principale).

# Messa in quarantena di un agente

Una volta messo in quarantena, un agente viene isolato dal traffico di rete in entrata o in uscita da CA Process Automation. Non è possibile eseguire gli operatori su un agente in quarantena. Mettere in quarantena un agente quando si desidera impedire che diventi la destinazione di un operatore di CA Process Automation.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo Agenti.
3. Selezionare l'agente da mettere in quarantena, quindi fare clic su Blocca.
4. Fare clic con il tasto destro del mouse sull'agente, quindi selezionare Quarantena. Il modificatore di quarantena viene aggiunto all'icona di base dell'agente bloccato.

5. Fare clic su Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che chiede se si desidera salvare le modifiche.

6. Fare clic su Sì.

   Il modificatore di quarantena viene visualizzato per il touchpoint o il gruppo host associato all'agente in quarantena.

# Rimozione di un agente dalla quarantena

Dopo che è trascorso il periodo di quarantena, rimuovere l'agente dalla quarantena.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione ed espandere il modo Agenti.
2. Fare clic sull'agente in quarantena per cui si desidera rimuovere la quarantena e fare clic su Blocca.
3. Fare clic con il tasto destro del mouse sull'agente, quindi fare clic su Rimuovi quarantena.
4. Fare clic su Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che chiede se si desidera salvare le modifiche.
5. Fare clic su Sì.

   Il modificatore del blocco per l'icona di base dell'agente viene rimosso. I modificatori di quarantena per l'agente e il touchpoint associato o per le icone di base del gruppo host vengono sostituiti dal modificatore dell'icona attivo.

# Ridenominazione di un agente

Per impostazione predefinita, durante il processo di installazione di un agente il nome dell'agente è il nome host. È possibile rinominare l'agente. Ad esempio, è possibile sostituire l'FQDN per l'host con Agent-*host_name*.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione ed espandere Agenti nel riquadro Browser di configurazione.
2. Selezionare l'agente da rinominare e fare clic su Blocca.
3. Fare clic con il tasto destro del mouse sull'agente e selezionare Rinomina.
4. Digitare il nuovo nome.
5. Fare clic su Salva.
6. Selezionare l'agente e fare clic su Sblocca.

# Identificazione del percorso di installazione di un agente

È possibile identificare il percorso di installazione dell'agente. Il percorso predefinito per un sistema operativo Windows 7 è:

```
C:\Program Files (x86)\CA\Pam Agent\PAMAgent
```

**Attenersi alla seguente procedura:**

Utilizzare lo script seguente per identificare il percorso di installazione dell'agente:

```
echo %C2OHOME%
```

Lo script restituisce il percorso di installazione completo dell'agente CA Process Automation.

**Nota:** Questo script suppone che si sia definito C2OHOME come variabile di ambiente.

# Gestire la rimozione di autorizzazioni di un host con un agente

Quando si riceve l'avviso che l'azienda intende sostituire l'hardware in cui sono installati gli agenti, si consiglia di attenersi alla seguente procedura per ridurre al minimo l'impatto. Questo processo riassegna i touchpoint originali per gli agenti installati sul nuovo hardware. La riassegnazione consente ai processi che si basano su questi touchpoint di continuare l'esecuzione senza modifiche.

Di seguito sono descritti due scenari comuni:

- I vecchi host vengono rimossi e quindi vengono aggiunti i nuovi host. Questa procedura è comune quando vengono riassegnati gli indirizzi IP.
- Il nuovo host viene aggiunto e quindi il vecchio host viene rimosso.

Nel caso in cui si intenda rimuovere i vecchi host prima della distribuzione di quelli nuovi, considerare l'approccio seguente:

1. Eseguire le seguenti operazioni prima che un host venga rimosso dalla rete:
   a. Identificare il nome dell'agente in CA Process Automation relativo all'host per cui si stanno revocando le autorizzazioni.

      Il riquadro Agenti nel browser di configurazione elenca tutti gli agenti con il loro stato.
   b. Identificare i touchpoint associati all'agente destinati all'eliminazione.

      Nel riquadro Agenti nel browser di configurazione, selezionare l'agente e fare clic sulla scheda Touchpoint associati per visualizzare l'elenco dei touchpoint da valutare per la riassegnazione.
   c. Disinstallare il software dell'agente dall'host a cui sono state revocate le autorizzazioni o che è stato reimpiegato per altri scopi.
2. Installare il software dell'agente sull'host che sostituisce l'host a cui è sono state revocate le autorizzazioni.
3. Associare i touchpoint interessati al nuovo agente.
4. Rimuovere da CA Process Automation l'agente relativo all'host a cui sono state revocate le autorizzazioni.

   Nel riquadro Agenti nel browser di configurazione, fare clic con il tasto destro del mouse sull'agente, selezionare Blocca, quindi fare clic con il tasto destro e selezionare Elimina.

Nel caso in cui i nuovi host vengano portati nella rete prima che i vecchi host siano eliminati, considerare l'approccio seguente:

1. Installare un agente su ogni nuovo host.
2. Associare i touchpoint interessati ai nuovi agenti.
3. Usare Rimozione degli agenti in blocco per rimuovere gli agenti che sono stati sostituiti.

**Ulteriori informazioni:**

Rimozione degli agenti selezionati in blocco (a pagina 217)
Rimozione in blocco dei touchpoint vuoti inutilizzati (a pagina 236)
Associare un touchpoint a un altro agente (a pagina 235)

## Eliminazione di un agente

Quando non si desidera più un agente installato, disinstallarlo dall'host. Eliminare quindi l'agente dal riquadro Agenti.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Espandere Agenti e verificare che l'agente di destinazione sia sbloccato e non in quarantena.
3. Selezionare l'agente di destinazione e fare clic su Elimina.

   Verrà visualizzata una finestra di dialogo di conferma.
4. Fare clic su OK.
5. Fare clic su Salva.
6. Selezionare Dominio e fare clic su Sblocca.

## Rimozione degli agenti selezionati in blocco

Quando ai server utilizzati per gli agenti vengono revocate le autorizzazioni, è possibile rimuovere in blocco i riferimenti di CA Process Automation a questi agenti non attivi. È quindi possibile rimuovere, in blocco, i touchpoint vuoti associati.

Quando la sostituzione dei server viene eseguita con una subnet alla volta, è possibile selezionare gli agenti associati per la rimozione specificando una ricerca basata su CIDR. Se i server a cui sono state revocate le autorizzazioni dispongono di un modello comune nei propri nomi host, è possibile selezionare gli agenti da rimuovere in base a un modello specificato che soddisfi i criteri.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse su Dominio e selezionare Blocca.
3. Fare clic con il pulsante destro del mouse su Dominio e selezionare Rimozione agente in blocco.
4. Immettere i criteri di ricerca in uno dei seguenti modi:
   - Selezionare Cerca per modello di indirizzo IP e immettere una subnet nel formato CIDR contenente gli indirizzi IP di destinazione.
   - Selezionare Cerca per modello nome host e immettere un'espressione di ricerca che includa il nome di dominio, ad esempio *.*mycompany*.com.
   - Selezionare uno dei modelli, ma lasciare il campo di ricerca vuoto.

5. Fare clic su Cerca.

   La tabella Agenti visualizza tutti gli agenti che soddisfano i criteri di ricerca, ma solo gli agenti non attivi possono essere selezionati per la rimozione.

6. Tra gli agenti inattivi visualizzati, selezionare gli agenti da rimuovere e fare clic su Elimina.

   Un messaggio di conferma che indica il numero di agenti selezionato chiede se continuare o annullare.

7. Selezionare Continua.

   Gli agenti selezionati vengono rimossi dal dominio e la modifica al dominio viene salvata automaticamente.

8. Fare clic con il pulsante destro del mouse su Dominio e selezionare Sblocca.

**Ulteriori informazioni:**

Rimozione in blocco dei touchpoint vuoti inutilizzati (a pagina 236)
Blocco del dominio (a pagina 137)
Gestire la rimozione di autorizzazioni di un host con un agente (a pagina 215)

# Avvio di un agente

Utilizzare il metodo di avvio o riavvio dell'agente per il sistema operativo sull'host che comprende l'agente.

### Avvio o riavvio di un agente su un host di Microsoft Windows

I passaggi seguenti si applicano a qualsiasi agente nel dominio di CA Process Automation che risiede su un host con un sistema operativo Windows.

**Attenersi alla procedura seguente:**

1. Accedere all'host di Windows su cui è installato un agente.
2. Dal menu Start, selezionare Programmi, CA, Agente CA Process Automation, Avvia servizio dell'agente.
3. Disconnettersi dall'host.

### Avvio o riavvio di un agente su un host di Linux

I passaggi seguenti si applicano a qualsiasi agente nel dominio di CA Process Automation che risiede su un host con un sistema operativo UNIX o Linux.

**Attenersi alla procedura seguente:**

1. Accedere all'host di UNIX o Linux su cui è installato un agente.
2. Modificare le directory in:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Eseguire il comando riportato di seguito:

   ```
   ./c2oagtd.sh start
   ```

   L'agente viene riavviato.

# Arresto di un agente

È possibile arrestare un agente di CA Process Automation in esecuzione su un host di UNIX o Linux.

### Arresto di un agente su un host di Microsoft Windows

I passaggi seguenti si applicano a qualsiasi agente nel dominio di CA Process Automation che risiede su un host con un sistema operativo Windows.

**Attenersi alla procedura seguente:**

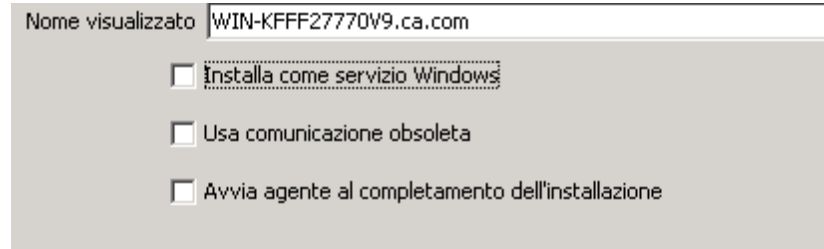
1. Accedere all'host di Windows su cui è installato un agente.
2. Dal menu Start, selezionare Programmi, CA, Agente CA Process Automation, Arresta servizio agente.
3. Disconnettersi dall'host.

### Arresto di un agente su un host Linux

I passaggi seguenti si applicano a qualsiasi agente nel dominio di CA Process Automation che risiede su un host con un sistema operativo UNIX o Linux.

**Attenersi alla procedura seguente:**

1. Accedere all'host di UNIX o Linux su cui è installato un agente.
2. Modificare le directory in:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Eseguire il comando riportato di seguito:

   ```
   ./c2oagtd.sh stop
   ```

   L'esecuzione dell'agente si arresta.

# Informazioni sulla comunicazione degli agenti

Le comunicazioni degli agenti vengono configurate quando si installa un agente. Per impostazione predefinita, i nuovi agenti utilizzano la nuova comunicazione semplificata. La casella di controllo Usa comunicazione obsoleta è deselezionata.

Gli agenti aggiornati utilizzano la comunicazione obsoleta. È possibile riconfigurare questa impostazione senza reinstallare l'agente.

Nome visualizzato WIN-KFFF27770V9.ca.com

Installa come servizio Windows

Usa comunicazione obsoleta

Avvia agente al completamento dell'installazione

**Comunicazione semplificata**

La comunicazione semplificata utilizza i socket Web e HTTP per produrre una connessione unidirezionale persistente dall'agente all'orchestrator. CA Process Automation utilizza una porta standard (80 o 443) che consente una connessione veloce tra i componenti.

**Comunicazione non più in uso**

La comunicazione obsoleta, che utilizza più porte, non si integra facilmente con il firewall o il router NAT come la comunicazione semplificata. Le connessioni inizializzate dall'orchestrator utilizzate nella comunicazione obsoleta non sono così efficienti come le connessioni permanenti utilizzate nella comunicazione semplificata.

## Configurazione degli agenti per l'utilizzo della comunicazione semplificata

È necessario reinstallare gli agenti esistenti per passare dalla comunicazione obsoleta a quella semplificata. È possibile eseguire questa azione per tutti gli agenti una volta completati l'aggiornamento a CA Process Automation 04.2.00 e l'installazione e la configurazione dell'utilità di bilanciamento del carico NGINX.

Reinstallare ogni agente come descritto in Installazione interattiva di un agente (a pagina 204). Per impostazione predefinita, la casella di controllo Usa comunicazione obsoleta è deselezionata. In questo modo, l'agente viene installato per utilizzare la comunicazione semplificata.

L'agente crea connessioni al socket Web e invia i dettagli di connessione a tutti i nodi dell'orchestrator. Gli orchestrator utilizzano questa connessione permanente al socket Web per inviare richieste o aggiornamenti all'agente, se necessario.

## Configurazione degli agenti per l'utilizzo della comunicazione non più in uso

Gli agenti installati con CA Process Automation 4.2 utilizzano la comunicazione semplificata per impostazione predefinita. Eventualmente, è possibile ripristinare la comunicazione obsoleta per l'agente.

In presenza di un ambiente con firewall abilitato, riconfigurare l'uso della porta di firewall prima di passare dalla comunicazione semplificata alla comunicazione obsoleta. Le porte Jetty utilizzate per la comunicazione semplificata sono le porte standard 80 e 443, rispettivamente per HTTP e HTTPS. Le porte Tomcat utilizzate nella comunicazione obsoleta sono 8080 e 8443. Per ulteriori informazioni sulle porte di agente, consultare l'argomento Porte utilizzate da un agente nella *Guida all'installazione*.

**Attenersi alla procedura seguente:**

1. Verificare che l'agente sia in esecuzione.

   Se il riquadro Agenti visualizza un agente di CA Process Automation non attivo, è possibile avviare l'agente. Consultare Come avviare o arrestare un agente.

2. Fare clic sulla scheda Configurazione ed espandere Agenti nel riquadro Browser di configurazione.

3. Selezionare l'agente di cui modificare la comunicazione e fare clic su Blocca.

4. Selezionare la scheda Proprietà per l'agente selezionato.

5. Selezionare la casella di controllo Usa comunicazione non più in uso.

6. Selezionare l'agente e fare clic su Sblocca.

7. Fare clic Sì nella finestra di dialogo Dati non salvati per salvare le modifiche.

L'agente termina la connessione con socket Web. In seguito all'interruzione della connessione con socket Web, l'agente utilizza la comunicazione non più in uso.

# Capitolo 9: Amministrazione dei touchpoint

I touchpoint eseguono il mapping di nomi simbolici su orchestrator e agenti. I touchpoint vengono utilizzati per identificare l'orchestrator o l'agente in un ambiente. Viene fornito un livello tra CA Process Automation e la topologia di rete che consente la configurazione degli operatori di CA Process Automation senza specificare esplicitamente le informazioni sull'host.

La configurazione della categoria di un operatore specifica il touchpoint su cui eseguire l'operatore. Un utente che configura un operatore di CA Process Automation seleziona un nome da un elenco di touchpoint configurati per eseguire gli operatori nella stessa categoria dell'operatore di riferimento. Questo riferimento indiretto consente di sostituire gli host in fase di runtime. Consente inoltre di definire più ambienti di CA Process Automation in cui gli stessi touchpoint sono mappati su host reali differenti.

Questa sezione contiene i seguenti argomenti:



## Strategia di implementazione dei touchpoint

Un *touchpoint* è una rappresentazione logica specifica dell'ambiente di una o più risorse gestite. Una *risorsa gestita* è un agente o un orchestrator su cui si eseguono gli operatori di un processo. Per eseguire un operatore su un agente specifico o sul relativo failover, è necessario specificare come destinazione il touchpoint mappato.

Gli amministratori del contenuto creano touchpoint per destinazioni di processo nell'ambiente di progettazione dopo aver completato i piani di processo, ma prima di avviare il processo di progettazione. I responsabili di progettazione dei contenuti creano il processo, in cui gli operatori utilizzano come destinazione i touchpoint creati. I responsabili di progettazione dei contenuti verificano il processo e lo inseriscono nel pacchetto per la transizione all'ambiente di produzione.

Prima di trasferire il processo, si creano touchpoint analoghi che associano agenti di produzione all'ambiente di produzione. In altre parole, nell'ambiente di produzione si creano nomi di touchpoint o di touchpoint proxy uguali a quelli utilizzati nell'ambiente di progettazione. La creazione dei touchpoint consente agli operatori nel processo trasferito di continuare a utilizzare gli stessi touchpoint come destinazioni di operatore.

Considerare il seguente processo:

1. Ottenere una versione di test del sistema esterno o dell'attività che si desidera utilizzare come destinazione.

   Gli esempi di entità esterne comprendono un'applicazione Service Desk, un database di produzione o un sistema di backup.

2. Installare un agente sull'host con la versione di test dell'entità che si pianifica di utilizzare come destinazione.

   Se non è possibile, creare una connessione SSH da un host agente all'host con la destinazione. Creare quindi un touchpoint proxy.

3. Mappare un touchpoint (o touchpoint proxy) sull'agente nell'ambiente di progettazione che esegue la copia di test del sistema esterno utilizzato come destinazione.

4. I responsabili di progettazione eseguono e verificano il processo, mentre gli operatori nel processo utilizzano come destinazione quel touchpoint per il test.

5. Durante la transizione di un processo all'ambiente di produzione, procedere come segue per ciascuna destinazione che sia un touchpoint agente:

   a. Identificare uno o più host che eseguono l'applicazione, il database o il sistema sulla destinazione.

   b. Installare un agente su ciascun host identificato.

   c. Creare un touchpoint che associa ogni agente di destinazione potenziale all'ambiente di produzione. Assegnare al touchpoint lo stesso nome utilizzato nell'ambiente di progettazione.

6. Durante la transizione di un processo, procedere come segue per ciascuna destinazione che sia un touchpoint proxy:

   a. Identificare l'host remoto che sta eseguendo l'applicazione, il database o il sistema di destinazione.

   b. Installare un agente su un host disponibile.

   c. Creare una connessione SSH dall'host agente all'host remoto.

   d. Creare un touchpoint proxy che associ l'host agente con l'ambiente di produzione. Assegnare al touchpoint proxy lo stesso nome utilizzato per il touchpoint proxy nell'ambiente di progettazione.

# Configurazione di touchpoint per la progettazione e la produzione

Un operatore che utilizza come destinazione un touchpoint può essere eseguito sia nell'ambiente di progettazione, sia in quello di produzione senza apportare modifiche al campo Destinazione. A tale scopo, viene definito lo stesso nome di touchpoint in ciascun ambiente.

È possibile impostare i touchpoint per la progettazione e la produzione una volta soddisfatti i seguenti prerequisiti:

- Installare agenti sugli host che verranno utilizzati come destinazione dal processo nell'ambiente di progettazione.
- Installare agenti sugli host che verranno utilizzati come destinazione dal processo nell'ambiente di produzione.

**Attenersi alla procedura seguente:**

1. Aggiungere un touchpoint nell'ambiente di progettazione (a pagina 226).
2. Configurare le proprietà per il touchpoint di progettazione (a pagina 226).
3. Aggiungere un touchpoint di produzione con lo stesso nome (a pagina 227).
4. Configurare il modo in cui gli operatori selezionano l'agente di destinazione (a pagina 229).
5. Configurare le proprietà per il touchpoint di produzione (a pagina 230).

## Aggiunta di un touchpoint nell'ambiente di progettazione

Un touchpoint associa un agente a un ambiente. È possibile aggiungere un touchpoint e associarlo a un agente installato su un host che si desidera utilizzare come destinazione durante le fasi di progettazione e test.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio nel browser di configurazione.
3. Selezionare l'ambiente utilizzato per la progettazione, quindi fare clic su Blocca.
4. Fare clic con il pulsante destro del mouse sull'ambiente, quindi fare clic su Aggiungi touchpoint.
5. Immettere un nome per il nuovo touchpoint nel campo Nome touchpoint della finestra di dialogo Aggiungi touchpoint:*ambiente*.
6. Selezionare l'agente installato sull'host che si desidera utilizzare come destinazione con questo touchpoint.
7. Fare clic su Aggiungi, quindi su Salva nella barra dei menu e infine fare clic con il pulsante destro del mouse sull'ambiente e selezionare Sblocca.
8. Visualizzare il touchpoint aggiunto nel nodo Tutti i touchpoint per l'ambiente di progettazione. Visualizzare la riga aggiuntiva nella scheda Dati touchpoint.

**Ulteriori informazioni:**

Configurazione delle proprietà per il touchpoint di progettazione (a pagina 226)
Configurazione delle proprietà dei touchpoint proxy (a pagina 249)

## Configurazione delle proprietà per il touchpoint di progettazione

Configurare le proprietà di un touchpoint in base all'ambiente. Per i touchpoint associati a un ambiente di progettazione, è possibile il ripristino manuale degli operatori. Questa impostazione offre la possibilità di una migliore risoluzione dei problemi. In genere, la protezione touchpoint utilizza come destinazione host di importanza strategica e non è applicabile a qualsiasi host agente utilizzato in fase di progettazione.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse sull'ambiente con i touchpoint da configurare, quindi selezionare Blocca.
3. Espandere l'ambiente, quindi espandere Tutti i touchpoint.

4. Selezionare il touchpoint da configurare, quindi fare clic sulla scheda Proprietà.
5. Impostare la proprietà Ripristino automatico degli operatori per consentire il ripristino manuale degli operatori. Questa impostazione permette di controllare in modo ottimale il ripristino degli operatori quando richiesto.
6. Se il touchpoint è protetto da una policy Protezione touchpoint attiva, abilitare la proprietà Protezione touchpoint.

   La proprietà, una volta abilitata, applica la policy adatta che specifica gli utenti autorizzati all'esecuzione degli operatori sulla destinazione corrente.
7. Fare clic su Salva.
8. Fare clic con il pulsante destro del mouse sull'ambiente, quindi selezionare Sblocca.

## Aggiunta di un touchpoint di produzione con lo stesso nome

Quando i responsabili di progettazione dei contenuti immettono nomi di touchpoint nel campo Destinazione per gli operatori, l'operatore viene eseguito sull'agente associato al touchpoint nell'ambiente di progettazione.

Un nome touchpoint deve essere univoco all'interno di un ambiente. Due ambienti possono avere touchpoint diversi con lo stesso nome. Lo scenario seguente, in cui esistono due touchpoint distinti chiamati TP-125, è valido.

- TP-125 associato ad agent-1 e all'ambiente di progettazione
- TP-125 associato ad agent-2 e all'ambiente di produzione

Gli agenti non sono specifici di un ambiente. È possibile associare due touchpoint con lo stesso nome in ambienti diversi allo stesso agente.

Quando un processo viene trasferito in un altro ambiente, ciascun operatore deve essere eseguito su un agente utilizzato nell'ambiente di importazione. Per preparare l'uso di un processo importato, procedere come segue:

1. Identificare ogni touchpoint utilizzato come destinazione da un operatore in un processo eseguito nell'ambiente di progettazione. Il processo può essere nella fase di pianificazione o pronto per l'esportazione.
2. Per ciascun touchpoint identificato, individuare due agenti appropriati utilizzati nell'ambiente di produzione su cui è possibile eseguire l'operatore. L'associazione di due agenti invece di uno è consigliabile ai fini dell'alta disponibilità.
3. Nell'ambiente di produzione, creare un touchpoint con lo stesso nome del touchpoint identificato. Associarlo agli agenti appropriati utilizzati nell'ambiente di produzione. La procedura seguente descrive questo passaggio.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse sull'ambiente di produzione nel riquadro Browser di configurazione, quindi fare clic su Blocca.
3. Fare clic con il pulsante destro del mouse sull'ambiente di produzione, quindi fare clic su Aggiungi touchpoint.
4. Immettere il nome di touchpoint utilizzato nell'ambiente di progettazione. Immettere il nome nel campo Nome touchpoint della finestra di dialogo Aggiungi Touchpoint:*ambiente di produzione*.
5. Selezionare i due agenti individuati in precedenza e utilizzabili come destinazione con questo touchpoint.
6. Fare clic su Aggiungi, quindi su Salva nella barra dei menu e infine fare clic con il pulsante destro del mouse sull'ambiente e selezionare Sblocca.
7. Visualizzare il touchpoint aggiunto nel nodo Tutti i touchpoint per l'ambiente di progettazione. Visualizzare la riga aggiuntiva nella scheda Dati touchpoint.

**Nota:** Se sono stati associati più agenti al touchpoint nell'ambiente di destinazione, è necessario configurare le modalità di selezione con gli operatori dell'agente di destinazione.

**Ulteriori informazioni:**

Configurazione di come gli operatori selezionano l'agente di destinazione (a pagina 229)

## Configurazione di come gli operatori selezionano l'agente di destinazione

È possibile associare più agenti allo stesso touchpoint. Quando un operatore utilizza come destinazione tale touchpoint, l'operatore può selezionare un agente specifico o selezionare un agente in modo casuale. Per impostazione predefinita, l'operatore seleziona il primo agente associato al touchpoint.

È possibile configurare come gli operatori selezionano l'agente di esecuzione.

- Per fornire agli operatori le istruzioni in modo da selezionare l'agente preferito, assegnare a tale agente la priorità 1. Assegnare la priorità 2 all'agente di backup.
- Per fornire agli operatori le istruzioni in modo da selezionare l'agente in modo casuale, assegnare la priorità 1 a tutti gli agenti.

È possibile configurare come gli operatori selezionano l'host di destinazione assegnando le priorità agli agenti associati.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere Dominio, selezionare l'ambiente da configurare, quindi fare clic su Blocca.
3. Espandere l'ambiente. In Tutti i touchpoint, fare clic sul touchpoint agente che si desidera configurare.

   La scheda Agenti visualizza l'elenco degli agenti mappati sul touchpoint selezionato. Ogni agente è elencato con un numero di priorità che riflette l'ordine in cui è stato aggiunto.
4. Esaminare le impostazioni di priorità visualizzate ed effettuare una delle seguenti operazioni:
   - Per il bilanciamento del carico, assegnare lo stesso numero a ogni agente potenzialmente attivo. Ad esempio, assegnare 1.
   - Per il backup, assegnare 1 all'agente da utilizzare come destinazione con il touchpoint. Assegnare 2 all'agente di backup che si occuperà dell'operazione solo se l'agente con priorità alta diventa non attivo.
   - Per entrambi, assegnare 1 agli agenti che partecipano al bilanciamento del carico e assegnare un numero maggiore all'agente o agli agenti che fungono come backup.
5. Fare clic su Salva.
6. Selezionare l'ambiente, quindi fare clic su Sblocca.

## Configurazione delle proprietà per il touchpoint di produzione

È possibile configurare le proprietà di un touchpoint in base all'ambiente associato. In un ambiente di produzione, se è abilitato il ripristino automatico degli operatori, si riduce il tempo richiesto per ripristinare l'esecuzione di un processo quando un operatore con processi ripristinabili non riesce. La protezione touchpoint è applicabile solo per host con un valore alto nell'ambiente di produzione. Pertanto, impostare questa proprietà a seconda se si dispone di una policy di protezione touchpoint per gli agenti associati a tale touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse sull'ambiente con i touchpoint da configurare, quindi selezionare Blocca.
3. Espandere l'ambiente, quindi espandere Tutti i touchpoint.
4. Selezionare il touchpoint da configurare, quindi fare clic sulla scheda Proprietà.
5. Impostare la proprietà Ripristino automatico degli operatori per ripristinare gli operatori in modo automatico.

   Questa impostazione attenua l'impatto dei problemi di rete sugli utenti dell'ambiente di produzione.
6. Se gli agenti di produzione associati al touchpoint sono definiti in una policy di protezione touchpoint, abilitare la proprietà Protezione touchpoint.

   La proprietà, una volta abilitata, applica la policy adatta che specifica gli utenti autorizzati all'esecuzione degli operatori su questi agenti.
7. Fare clic su Salva.
8. Fare clic con il pulsante destro del mouse sull'ambiente, quindi selezionare Sblocca.

# Aggiunta di uno o più touchpoint

È possibile aggiungere un touchpoint alla volta.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio nel browser di configurazione.
3. Fare clic con il pulsante destro del mouse sull'ambiente da configurare, quindi fare clic su Blocca.
4. Fare clic con il pulsante destro del mouse sull'ambiente, quindi fare clic su Aggiungi touchpoint.

5. Immettere un nome per il nuovo touchpoint nel campo Nome touchpoint della finestra di dialogo Aggiungi touchpoint:*ambiente*.
6. Selezionare un oggetto da associare al touchpoint dall'elenco a discesa. Selezionare:
   - Un orchestrator
   - Un agente
   - Più agenti
7. Fare clic su Aggiungi, quindi su Salva nella barra dei menu e infine fare clic con il pulsante destro del mouse sull'ambiente e selezionare Sblocca.
8. Visualizzare i touchpoint aggiunti nel nodo Tutti i touchpoint per l'ambiente selezionato. Visualizzare la riga aggiuntiva nella scheda Dati touchpoint.

**Ulteriori informazioni:**

Configurazione delle proprietà per il touchpoint di progettazione (a pagina 226)
Configurazione delle proprietà dei touchpoint proxy (a pagina 249)

# Aggiunta di uno o più agenti a un touchpoint esistente

Aggiungere uno o più agenti a un touchpoint esistente. Si consiglia di aggiungere più di un agente a ciascun touchpoint associato al proprio ambiente di produzione. Se un agente non è disponibile, un operatore che utilizza come destinazione il touchpoint può essere eseguito su un altro agente associato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo Dominio nel riquadro Browser di configurazione, selezionare un ambiente, quindi fare clic su Blocca.

3. Se un touchpoint non esiste, crearne uno:
    a. Espandere il nodo Agenti.
    b. Identificare un agente che viene eseguito nell'ambiente bloccato. Fare clic con il pulsante destro del mouse sull'agente, selezionare Configura touchpoint su, quindi selezionare l'ambiente bloccato.

       Viene visualizzata la finestra di dialogo Aggiungi touchpoint agente.
    c. Immettere il nome del touchpoint rispettivo e fare clic su OK.
4. Per aggiungere uno o più agenti a un touchpoint esistente:
    a. Espandere Tutti i touchpoint per l'ambiente selezionato, selezionare il touchpoint di destinazione, quindi fare clic su Aggiungi.
    b. Selezionare uno o più agenti attivi eseguiti nell'ambiente bloccato, quindi fare clic su Aggiungi. (Gli agenti attivi vengono visualizzati in verde.)

       I nuovi agenti da associare al touchpoint selezionato sono visualizzati nell'elenco della scheda Agenti.
    c. Fare clic su Salva.

       Adesso il touchpoint selezionato è associato agli agenti aggiuntivi.
5. Fare clic con il pulsante destro del mouse sull'ambiente bloccato, quindi selezionare Sblocca.
6. Fare clic su Sì nel prompt per salvare le modifiche.

**Nota:** Se sono stati associati più agenti al touchpoint nell'ambiente di destinazione, configurare il modo in cui gli operatori selezionano l'agente di destinazione.

**Ulteriori informazioni:**

Configurazione di come gli operatori selezionano l'agente di destinazione (a pagina 229)

# Aggiunta in blocco di touchpoint per gli agenti

È possibile aggiungere in blocco touchpoint per i nuovi agenti specificando i modelli per i nomi o gli indirizzi IP dell'host agente. Ogni agente con un nome host o un indirizzo IP che corrisponde a un modello specificato viene configurato automaticamente con un touchpoint. Il nome touchpoint è lo stesso del nome agente visualizzato. Un *modello di assegnazione automatica* è un modello di nome host indicato come un'espressione regolare o una subnet di indirizzo IP espresso in notazione CIDR.

È possibile configurare modelli di assegnazione automatica differenti per ciascun ambiente oppure modelli di assegnazione automatica uguali o sovrapponibili tra gli ambienti. I touchpoint sono specifici dell'ambiente. Gli agenti non sono specifici dell'ambiente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere Dominio nel Browser di configurazione.
3. Fare clic con il tasto destro del mouse sull'ambiente da configurare, quindi fare clic su Blocca.
4. Fare clic sulla scheda Ammissione automatica.
5. Per ciascun modello di indirizzo IP, attenersi ai passaggi seguenti. Quindi, utilizzare le frecce su o giù per ordinare l'elenco della ricerca.
    a. Fare clic su Aggiungi nell'area Modelli di indirizzo IP.

       Viene visualizzato un campo di immissione.

    b. Immettere una subnet IPv4 utilizzando la notazione CIDR.

       **Nota:** CA Process Automation utilizza la corrispondenza di modelli CIDR per i requisiti di ammissione automatica. Ad esempio, il modello CIDR 155.32.45.0/24 corrisponde agli indirizzi IP compresi nell'intervallo da 155.32.45.0 a 155.32.45.255.
6. Per ciascun modello di nome host, attenersi ai passaggi seguenti. Quindi, utilizzare le frecce su o giù per ordinare l'elenco della ricerca.
    a. Fare clic su Aggiungi nell'area Modelli di nome host.
    b. Immettere un modello di nome host.

       **Nota**: il nome host dell'orchestrator/agente viene confrontato con le espressioni regolari specificate. Ad esempio, se il modello specificato è ca\.com$, vengono aggiunti tutti gli agenti/orchestrator i cui nomi host terminano con ca.com.

7. Fare clic con il pulsante destro del mouse sull'ambiente, quindi fare clic su Sblocca.
8. Ripetere questa procedura per ciascun ambiente.

   Il dominio esegue la ricerca di un nuovo orchestrator e di nuovi agenti con indirizzi IP o nomi host corrispondenti ai modelli di assegnazione automatica per uno o più ambienti.

   Quando questi nuovi agenti vengono rilevati, il dominio crea un touchpoint per ciascuna corrispondenza e lo aggiunge automaticamente a ciascun ambiente. Il nome del touchpoint è il nome visualizzato dell'agente.

   Quando questo orchestrator viene rilevato, il dominio crea un touchpoint per tale orchestrator e lo aggiunge al primo ambiente corrispondente. Un orchestrator ha un solo touchpoint.

### Esempio di touchpoint aggiunti agli ambienti sulla base di modelli di assegnazione automatica degli agenti

Nell'esempio seguente, vengono definiti modelli di assegnazione automatica sovrapposti per due ambienti. Sono installati due agenti: l'indirizzo IP di uno di questi corrisponde a un modello di assegnazione automatica in un ambiente, mentre l'indirizzo IP dell'altro corrisponde ai modelli di assegnazione automatica in entrambi gli ambienti. Il risultato è l'aggiunta automatica di tre touchpoint.

- Ambiente1 ha il modello di ammissione automatica 155.32.45.0/24 (da 155.32.45.0 a 155.32.45.255)
- Ambiente2 ha il modello di ammissione automatica 155.32.45.32/27 (da 155.32.45.32 a 155.32.45.63)
- Vengono installati nuovi agenti con questi indirizzi:
  - 155.32.45.5 con nome visualizzato host1.mycompany.com
  - 155.32.45.50 con nome visualizzato host2.mycompany.com

Vengono aggiunti automaticamente i seguenti touchpoint sulla base dei modelli di assegnazione automatica:

- Nome touchpoint: host1.mycompany.com in Ambiente1
- Nome touchpoint: host2.mycompany.com in Ambiente1
- Nome touchpoint: host2.mycompany.com in Ambiente2

# Associare un touchpoint a un altro agente

Associare un touchpoint esistente a un altro agente nei casi seguenti:

- Un processo viene eseguito su un host messo in lista per essere rimosso dalla rete.

  Qui, il touchpoint è associato a un solo agente e tale agente è installato su un host pianificato per la revoca delle autorizzazioni. Se un touchpoint è associato a più agenti, non è richiesta alcuna azione.

- Un processo in esecuzione in un centro dati adesso deve essere eseguito in un altro centro dati.

  Qui, il processo fa riferimento a un touchpoint che deve essere associato a un agente installato su un host nel nuovo centro dati.

La modifica all'associazione dell'agente per un touchpoint selezionato comporta l'eliminazione dell'associazione dell'agente attuale e l'aggiunta di una nuova associazione dell'agente. Per eseguire un processo verificato su più host, associare lo stesso touchpoint di riferimento all'agente eseguito su ogni host di destinazione.

È possibile sostituire l'associazione dell'agente per un determinato touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere la struttura per visualizzare Tutti i touchpoint e selezionare il touchpoint di destinazione.

   La scheda Agenti nel riquadro principale elenca l'agente o gli agenti attualmente associati al touchpoint selezionato.

3. Selezionare l'agente con cui si desidera interrompere l'associazione e fare clic su Elimina.
4. Quando viene visualizzato il messaggio per la conferma dell'eliminazione, fare clic su OK.

   Il touchpoint agente viene rimosso dall'elenco.

5. Fare clic su Aggiungi.

   L'opzione Aggiungi riferimento agente a: *touchpointName* visualizza l'elenco di tutti gli agenti. Gli agenti attivi vengono visualizzati in verde.

6. Selezionare uno o più agenti attivi e fare clic su Aggiungi.

   Il nuovo agente da associare al touchpoint selezionato viene visualizzato nell'elenco della scheda Agenti.

7. Fare clic su Salva.

   Adesso il touchpoint selezionato è associato a un agente diverso.

**Ulteriori informazioni:**

Gestire la rimozione di autorizzazioni di un host con un agente (a pagina 215)

# Eliminazione di un touchpoint

È possibile eliminare un touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio e l'ambiente con il touchpoint.
3. Fare clic con il pulsante destro del mouse sull'ambiente con il touchpoint, quindi fare clic su Blocca.
4. Espandere Tutti i touchpoint e selezionare il touchpoint da eliminare.

   Viene visualizzata la scheda Agenti con l'elenco degli agenti associati al touchpoint.
5. Selezionare tutti gli agenti associati al touchpoint, quindi fare clic su Elimina.

   Viene visualizzato un messaggio di conferma.
6. Fare clic su Sì.

   Il touchpoint eliminato viene rimosso dall'elenco Tutti i touchpoint e dalla scheda Dati touchpoint.
7. Selezionare Dominio e fare clic su Sblocca.

# Rimozione in blocco dei touchpoint vuoti inutilizzati

La rimozione in blocco degli agenti può comportare la creazione di molti touchpoint vuoti. Se questi touchpoint vengono utilizzati nei processi attivi, è necessario riassegnarli ad altri agenti.

La rimozione dei touchpoint può avvenire a due livelli:

- Per rimuovere i touchpoint selezionati in più ambienti, avviare la rimozione dal menu di scelta rapida del dominio.

  È necessario essere amministratore di contenuto e disporre di diritti di amministratore di dominio.
- Per rimuovere i touchpoint selezionati in un solo ambiente, avviare la rimozione dal menu di scelta rapida dell'ambiente.

  È necessario disporre di diritti Amministratore del contenuto per l'ambiente selezionato per rimuovere i touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Bloccare il dominio o l'ambiente di destinazione. Se il dominio o l'ambiente di destinazione è già bloccato con modifiche non salvate, salvare le modifiche.
3. Fare clic con il pulsante destro del mouse sul dominio o sull'ambiente di destinazione e selezionare Rimozione touchpoint in blocco.

   Viene visualizzata la finestra di dialogo Rimozione touchpoint in blocco.
4. Fare clic su Cerca, oppure immettere un'espressione di ricerca del nome di un touchpoint e fare clic su Cerca.

   L'elenco restituito contiene solo i nomi e gli stati dei touchpoint vuoti corrispondenti ai criteri di ricerca immessi. Se la rimozione è stata avviata a livello di dominio, per ciascun touchpoint viene visualizzato anche l'ambiente.
5. Selezionare dall'elenco visualizzato i touchpoint da eliminare che non siano mappati su agenti, quindi fare clic su Elimina.

   Un messaggio di conferma definisce il numero di touchpoint destinati all'eliminazione.
6. Valutare il messaggio.
   - Se il numero visualizzato riflette il numero che si intendeva selezionare, fare clic su Continua per rimuovere tali touchpoint.
   - Se si è verificato un errore di selezione, fare clic su Annulla e ripetere i passaggi 4 e 5.

**Ulteriori informazioni:**

Rimozione degli agenti selezionati in blocco (a pagina 217)

# Ridenominazione di un touchpoint

La procedura per rinominare un touchpoint presenta dei prerequisiti solo quando l'operatore Esegui programma o l'operatore Esegui script viene eseguito sul touchpoint.

**Importante**. Gli operatori Esegui programma ed Esegui script nella categoria di esecuzione dei comandi fanno direttamente riferimento ai touchpoint in base al nome. Pertanto, prima di rinominare un touchpoint è necessario aggiornarne i riferimenti negli operatori Esegui programma ed Esegui script.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione ed espandere Dominio nel riquadro Browser di configurazione.
2. Selezionare l'ambiente appropriato, quindi fare clic su Blocca.
3. Espandere Tutti i touchpoint.
4. Fare clic con il pulsante destro del mouse sul touchpoint appropriato, quindi fare clic su Rinomina.
5. Immettere il nome del nuovo touchpoint agente.

   **Nota:** L'icona per i dati non salvati a sinistra della voce ricorda di salvare le modifiche. Fare clic su Salva o attendere il prompt di testo.
6. Selezionare l'ambiente bloccato, quindi fare clic su Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che richiede se salvare le modifiche.
7. Fare clic su Sì.

# Gestione dei gruppi touchpoint

Ogni touchpoint è un membro del gruppo predefinito denominato Tutti i touchpoint. Inoltre, è possibile creare propri gruppi denominati per raggruppare i touchpoint dal punto di vista logico o funzionale. Dal punto di vista logico, i gruppi touchpoint consentono di organizzare i touchpoint correlati e cercare più facilmente tra i touchpoint in un ambiente.

Dal punto di vista funzionale, i gruppi touchpoint consentono ai comandi e agli operatori di operare su tutti i touchpoint nel gruppo:

- Il comando Ricarica eseguito in un gruppo touchpoint aggiorna l'elenco di touchpoint per tutti i touchpoint all'interno del gruppo.
- Il comando Aggiorna eseguito su un gruppo touchpoint aggiorna le impostazioni di proprietà per tutti i touchpoint nel gruppo.
- Un operatore configurato per l'esecuzione in un gruppo in fase di runtime viene eseguito su ogni touchpoint nel gruppo.

Un gruppo touchpoint è attivo se almeno un touchpoint nel gruppo è attivo. Un gruppo touchpoint non è attivo se tutti i touchpoint nel gruppo sono inattivi. Se tutti i touchpoint in un gruppo sono attivi, l'icona del gruppo touchpoint è verde. Se solo alcuni touchpoint sono attivi, l'icona del gruppo touchpoint è gialla. Se tutti i touchpoint in un gruppo sono non attivi, l'icona del gruppo touchpoint è rossa.

L'utente deve disporre di autorizzazioni di amministratore di ambiente per creare un gruppo touchpoint in un ambiente.

# Informazioni sui gruppi touchpoint

Quando un dato operatore deve utilizzare come destinazione più touchpoint contemporaneamente, gli amministratori creano un gruppo touchpoint che può servire come destinazione di operatore. Ad esempio:

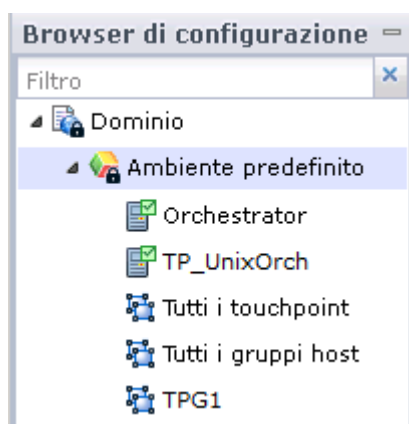
Quando gli amministratori eseguono la transizione della destinazione di un gruppo touchpoint nell'ambiente di produzione, creano un gruppo touchpoint nell'ambiente di produzione. Il nome touchpoint duplica il nome utilizzato nell'ambiente di progettazione. Gli amministratori associano gli agenti di produzione e gli orchestrator al gruppo touchpoint. Quando testano il processo, verificano tra l'altro che gli operatori che utilizzano un gruppo touchpoint come destinazione vengano effettivamente eseguiti su ciascun orchestrator e agente rappresentato da un touchpoint nel gruppo. Ad esempio:

## Creazione di un gruppo touchpoint con i touchpoint selezionati

Creare un gruppo touchpoint che può fungere da destinazione dell'operatore quando un determinato operatore deve utilizzare contemporaneamente più touchpoint come destinazione. Si aggiunge un gruppo touchpoint a livello di ambiente. Selezionare ciascun touchpoint per il gruppo dalla gerarchia di dominio. È possibile selezionare un touchpoint dell'orchestrator o un touchpoint agente, quindi utilizzare l'opzione Copia in per copiare il touchpoint selezionato in un gruppo touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio, selezionare l'ambiente da configurare, quindi fare clic su Blocca.
3. Creare un gruppo touchpoint:
    a. Fare clic con il pulsante destro del mouse su un ambiente, quindi selezionare Aggiungi nuovo gruppo.
    b. Nella finestra di dialogo Aggiungi gruppo touchpoint, immettere un nome per il gruppo touchpoint e fare clic su OK.

       Ad esempio, se il nome inserito è TPG1, il nome del nuovo gruppo viene visualizzato nell'ambiente selezionato in Tutti i gruppi host.

    c. Fare clic su Salva.

       **Nota:** non è possibile aggiungere correttamente un orchestrator a un gruppo touchpoint non salvato.

4. Copiare i touchpoint dell'orchestrator e i touchpoint dell'agente nel gruppo touchpoint. Ad esempio:

   a. Fare clic con il pulsante destro del mouse su un orchestrator, quindi selezionare Copia in, *group_name*.

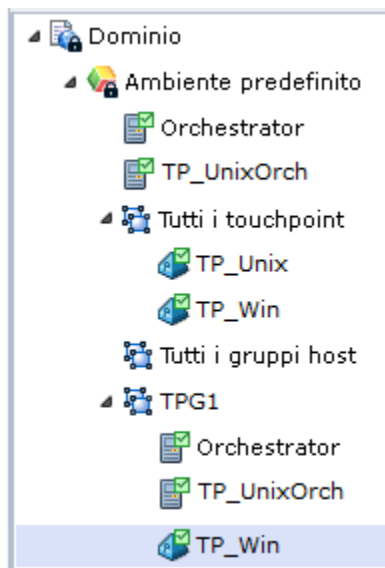
      L'orchestrator selezionato viene visualizzato nella gerarchia sotto al nome del gruppo touchpoint selezionato.

   b. Fare clic su Salva.

   c. Fare clic con il pulsante destro del mouse su un altro orchestrator, selezionare Copia in e scegliere lo stesso *group_name*.

   d. Fare clic su Salva.

   e. Espandere Tutti i touchpoint, fare clic con il pulsante destro del mouse su un touchpoint agente, selezionare Copia in e scegliere lo stesso *group_name*.

   Nell'esempio seguente il gruppo touchpoint TPG1 visualizza i contenuti di due touchpoint dell'orchestrator e di un touchpoint agente:

   


5. Selezionare l'ambiente, quindi selezionare Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che richiede se salvare le modifiche.

6. Fare clic su Sì.

**Ulteriori informazioni:**

Gestione dei gruppi touchpoint (a pagina 239)

## Eliminazione di un touchpoint da un gruppo touchpoint

L'eliminazione di un touchpoint da un gruppo touchpoint consente di rimuoverlo solo dal gruppo. L'eliminazione di un touchpoint dal gruppo Tutti i touchpoint consente di rimuoverlo dall'ambiente e da tutti gli altri gruppi touchpoint a cui era stato aggiunto. Gli amministratori del contenuto possono eliminare un touchpoint da un gruppo touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio, selezionare l'ambiente da configurare e fare clic su Blocca.
3. Espandere il gruppo touchpoint da configurare.
4. Selezionare il touchpoint da rimuovere dal gruppo e fare clic su Elimina.
5. Selezionare l'ambiente, quindi fare clic su Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che chiede se si desidera salvare le modifiche.
6. Fare clic su Sì.

## Eliminazione di un gruppo touchpoint

Gli amministratori del contenuto possono eliminare un gruppo touchpoint creato dall'utente e tutti i relativi touchpoint da un ambiente. Questa procedura non elimina il touchpoint da tutti gli altri gruppi nell'ambiente. È impossibile eliminare il gruppo di tutti i touchpoint.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il dominio, selezionare l'ambiente da configurare e fare clic su Blocca.
3. Fare clic con il pulsante destro del mouse sul gruppo touchpoint che si desidera rimuovere dall'ambiente, quindi fare clic su Elimina.
4. Selezionare l'ambiente, quindi fare clic su Sblocca.

   Viene visualizzata la finestra di dialogo Dati non salvati, che chiede se si desidera salvare le modifiche.
5. Fare clic su Sì.

# Capitolo 10: Amministrazione dei touchpoint proxy

Quando un operatore utilizza come destinazione un touchpoint proxy, l'operatore viene eseguito sull'host remoto che presenta una connessione SSH con l'host del touchpoint proxy. Sull'host remoto non è installato alcun software dell'agente. È possibile eseguire gli operatori su qualsiasi periferica con sistema operativo Windows o UNIX. Un touchpoint proxy riduce complessivamente le prestazioni, ma è utile quando il software dell'agente non può essere installato su un host di destinazione.

Per utilizzare un touchpoint proxy configurare un touchpoint di CA Process Automation da puntare a una destinazione remota e creare un utente SSH sul computer di destinazione.

Questa sezione contiene i seguenti argomenti:

# Prerequisiti dei touchpoint proxy

I touchpoint proxy possono essere creati tramite la configurazione di un touchpoint esistente per operare come touchpoint proxy su un computer remoto o su un'altra periferica. Un touchpoint può essere configurato come touchpoint proxy per un host con un ambiente operativo UNIX o Windows. I touchpoint proxy utilizzano SSH per eseguire le azioni sui computer di destinazione.

I prerequisiti per l'utilizzo di touchpoint proxy sono i seguenti:

- È necessario disporre di Java Virtual Machine (JVM) 1.6+ o versione successiva sull'host con il touchpoint da configurare come touchpoint proxy.
- Quando la destinazione di un touchpoint proxy è un computer UNIX, la shell Korn (ksh) deve essere installata sul computer di destinazione. Se mance nella destinazione, installare la shell Korn o creare un collegamento dalla shell Bash.
- Un account utente SSH deve essere specificato sul computer remoto utilizzato come destinazione da un touchpoint proxy.
- (Facoltativo) Per utilizzare l'autenticazione con chiave pubblica, è necessario creare una relazione di trust dall'host del touchpoint proxy al computer remoto di destinazione.

  **Importante.** Se si esegue questo passaggio, accertarsi di rispettare le istruzioni riportate nei requisiti specifici di CA Process Automation per la connettività SSH.
- In CA Process Automation, il touchpoint proxy deve essere configurato con le informazioni di autenticazione e le altre specifiche per l'host remoto.

**Ulteriori informazioni:**

Requisiti specifici di CA Process Automation per la connettività SSH (a pagina 247)
Creazione di una relazione di trust SSH con l'host remoto (a pagina 248)
Configurazione delle proprietà dei touchpoint proxy (a pagina 249)
Creare l'account utente SSH sull'host remoto del touchpoint proxy. (a pagina 248)

## Requisiti specifici di CA Process Automation per la connettività SSH

La connettività SSH può essere ottenuta tramite la creazione di un account utente SSH in ogni host di destinazione. Se si crea una relazione di trust facoltativa tra un host agente e un host remoto, vengono applicati alcuni requisiti specifici di configurazione di CA Process Automation.

Quando una richiesta a un host remoto viene elaborata, vengono lette le seguenti proprietà:

- Nome utente remoto.
- Password remota.
- Percorso delle chiavi SSH, se configurato.

CA Process Automation tenta una connessione SSH dall'host agente all'host remoto specificato nella richiesta. Il primo tentativo di accesso viene eseguito con le credenziali dell'account utente. Se il tentativo non riesce, viene eseguito un secondo tentativo tramite l'autenticazione con chiave. Per utilizzare l'autenticazione tramite chiave pubblica SSH con CA Process Automation, il nome del file di chiave privata deve corrispondere al nome dell'account utente. Se viene specificata una passphrase durante la creazione di chiavi, la passphrase deve corrispondere alla password dell'account utente. Di conseguenza, i due campi seguenti hanno una doppia funzione.

**Nome utente remoto**

È il nome utente per l'account utente utilizzato per l'autenticazione basata su credenziali SSH.

È inoltre il nome del file di chiave che archivia la chiave privata SSH nel percorso configurato come percorso delle chiavi SSH, se configurato.

**Password remota**

Indica la password per l'account utente utilizzata quando, per l'autenticazione, vengono utilizzate le credenziali SSH.

È anche la passphrase utilizzata quando la chiave pubblica SSH viene utilizzata per l'autenticazione.

Attenersi alle seguenti linee guida per la creazione di una relazione di trust dall'host locale all'host remoto:

- Inserire il nome dell'utente remoto per *user_name* quando si immette il comando seguente:

  ```
  ssh-keygen -t dsa -b 1024 -f user_name
  ```

- Immettere la password remota come passphrase.

## Creare l'account utente SSH sull'host remoto del touchpoint proxy.

La configurazione del touchpoint proxy consente di specificare il nome utente remoto e la password remota dell'account utente SSH utilizzato per accedere all'host remoto. L'account utente SSH deve disporre di autorizzazioni a livello di amministratore necessarie per l'esecuzione di operatori di CA Process Automation sul computer di destinazione. Valutare la definizione di uno stesso account utente per tutti i computer configurati in modo analogo a cui si accede come host remoti. Ad esempio, aggiungere l'account *pamuser*, con la stessa password, a ciascun host remoto.

Quando un touchpoint proxy stabilisce una connessione all'host remoto, crea una directory temporanea denominata c2otmp sul computer di destinazione. Su un computer UNIX, tale directory viene creata nella directory /home dell'utente SSH.

## Creazione di una relazione di trust SSH con l'host remoto

Se si desidera rendere disponibile l'autenticazione della chiave pubblica, creare una relazione di trust tra l'host del touchpoint proxy e l'host remoto di destinazione. Quindi, verificare la connettività SSH dal computer su cui è in esecuzione il touchpoint proxy al computer di destinazione. Creazione di una relazione di trust tra due computer host.

CA Process Automation utilizza l'autenticazione di chiave pubblica che si configura solo se l'autenticazione di utente/password non riesce.

Per creare una relazione di trust, utilizzare il programma ssh-keygen per generare la coppia di chiavi pubblica e privata. La chiave privata rimane sull'host con l'agente. Copiare la chiave pubblica per l'host remoto di destinazione che non dispone di agente.

**Attenersi alla procedura seguente:**

1. Generare una coppia di chiavi. Utilizzare il seguente comando, in cui *user_name* è il nome utente nell'account utente SSH creato sul computer di destinazione.

   ```
   ssh-keygen -t dsa -b 1024 -f user_name
   ```

   Viene richiesto di immettere una passphrase da utilizzare in seguito come password.

2. Specificare la passphrase per rispondere alla richiesta.

   Vengono creati il file di chiave privata denominato *user_name* e il file di chiave pubblica denominato <user_name>.pub.

3. Inserire il file di chiave privata denominato *user_name* in una delle seguenti posizioni:

   ■ La directory delle chiavi private è specificata nella configurazione del proxy.

     Si accede alla chiave da questa directory con qualsiasi host per cui non è previsto alcun file *target_host_name*/*user_name.*

   ■ La directory SshKeys/*target_host_name* è secondaria rispetto alla directory delle chiavi private specificata nel file di configurazione proxy. Si accede alla chiave privata da questa directory durante il tentativo di connessione di *user_name* a *target_host_name*.

     L'opzione Percorso chiavi SSH specifica la posizione per la directory delle chiavi private nella finestra di dialogo delle proprietà di touchpoint proxy.

4. Trasferire il file di chiave pubblica (*user_name*.pub) all'host di destinazione e spostarlo in un punto dove il daemon SSH possa trovarlo.

   Daemon SSH differenti seguono convenzioni diverse. Esaminare le opzioni ssh-keygen per informazioni sui requisiti di formattazione per il file della chiave pubblica.

5. Per OpenSSH, concatenare il file pubblico al file che contiene le chiavi autorizzate per user_name. Eseguire il seguente comando cat nell'host SSH di destinazione proxy:

   ```
   cat user_name.pub >> ~user_name/.ssh/authorized_keys
   ```

**Ulteriori informazioni:**

Requisiti specifici di CA Process Automation per la connettività SSH (a pagina 247)

# Configurazione delle proprietà dei touchpoint proxy

È possibile creare un touchpoint proxy riconfigurando un touchpoint agente esistente per utilizzare come destinazione il computer remoto specificato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il nodo Dominio, selezionare l'ambiente da configurare, quindi fare clic su Blocca.
3. In Tutti i touchpoint, selezionare il touchpoint agente da trasformare in touchpoint proxy.

4. Verificare che siano impostate le proprietà seguenti:
   - Ripristino automatico operatori
   - Protezione touchpoint

   Se non sono impostate, consultare la sezione Configurazione delle proprietà dei touchpoint (a pagina 226).

5. Selezionare la casella di controllo Touchpoint proxy.

   La selezione indica che questo touchpoint è un touchpoint proxy. Un touchpoint proxy viene mappato su un host remoto. Un host remoto in genere non ha agenti installati.

6. Configurare l'host remoto e i valori per l'autenticazione SSH. Completare i passaggi seguenti:

   a. Immettere il percorso assoluto o relativo sull'host agente su cui è archiviato il file di chiave privata nel campo Percorso chiavi SSH.

      I nomi del file di chiave privata (<user_name>) e del file di chiave pubblica (<user_name>.pub) corrispondono al nome utente remoto dell'account utente.

   b. Identificare l'host remoto con il nome di dominio completo o con l'indirizzo IP nel campo Host remoto.

      **Nota:** consultare la sezione Sintassi per nomi host DNS (a pagina 407).

   c. Immettere il nome utente con cui si esegue la connessione al daemon SSH sull'host di destinazione nel campo Nome utente remoto.

      L'account utente SSH deve disporre di autorizzazioni sufficienti per eseguire le attività di amministrazione nel computer di destinazione.

   d. Immettere la password dell'account utente associato al nome utente remoto.

      Questo valore viene utilizzato anche come passphrase se la connessione viene stabilita attraverso autenticazione SSH tramite chiave pubblica.

   e. Immettere il numero massimo di connessioni simultanee che è possibile aprire con il touchpoint proxy sull'host remoto di destinazione nel campo Numero massimo processi attivi.

      Una connessione SSH rimane aperta quando un programma o uno script vengono eseguiti nell'host di destinazione. Se impostato su 20 e si tenta di eseguire 40 script sull'host remoto contemporaneamente, si avvia solo l'esecuzione di 20 script. Gli script non avviati attendono in coda fino al completamento degli altri script, quindi vengono avviati.

   f. Selezionare il sistema operativo dell'host remoto di destinazione.

7. Fare clic su Salva.

8. Fare clic con il pulsante destro del mouse sull'ambiente, quindi selezionare Sblocca.

**Ulteriori informazioni:**

Configurazione delle proprietà per il touchpoint di progettazione (a pagina 226)
Aggiunta di uno o più touchpoint (a pagina 230)

# Utilizzare un touchpoint proxy

Quando un processo viene eseguito, gli operatori nel processo eseguono operazioni sugli host di destinazione. Per eseguire un operatore su un host remoto senza agenti, creare prima una connessione SSH da un host agente all'host remoto. Quando si crea un touchpoint e si seleziona un agente con una connessione a un host remoto, quel touchpoint diventa un touchpoint proxy. Quando un operatore specifica un touchpoint proxy come destinazione, l'operazione influisce sull'host remoto.

Per eseguire un'operazione in vari touchpoint proxy configurati in maniera analoga, è possibile raggruppare i touchpoint in un gruppo touchpoint. Quindi, specificare il gruppo touchpoint come destinazione durante la configurazione delle proprietà dell'operatore. In fase di runtime, l'operatore viene eseguito su tutti i touchpoint proxy nel gruppo.

**Ulteriori informazioni:**

Gestione dei gruppi touchpoint (a pagina 239)

# Capitolo 11: Amministrazione di gruppi host

CA Process Automation è in grado di eseguire gli operatori su una destinazione che non ha agenti o touchpoint quando si fa riferimento a tale destinazione in un gruppo host. Le progettazioni di contenuto possono specificare una destinazione tramite il relativo indirizzo IP o nome di dominio completo (FQDN).

**Nota:** consultare la sezione Sintassi per nomi host DNS (a pagina 407).

Quando lo stesso gruppo host si trova su più agenti, l'agente selezionato per l'esecuzione dell'operatore dipende dalla priorità dell'agente.

Questa sezione contiene i seguenti argomenti:



## Informazioni sui gruppi host

Un *gruppo host* rappresenta un gruppo di host, in genere con nomi o indirizzi IP simili, ciascuno dei quali può essere specificato in un operatore con il nome di dominio completo (FQDN) o l'indirizzo IP. Un gruppo host fa riferimento all'host come subnet di indirizzi IP, modelli di nome host o elenco di indirizzi IP specifici e FQDN.

I gruppi host forniscono accesso diretto, ovvero la possibilità di specificare un indirizzo IP o un nome di dominio completo (FQDN) in un operatore, anziché un nome di touchpoint o di touchpoint proxy. L'host a cui si fa riferimento in un gruppo host non necessita di associazioni di agenti o di touchpoint proxy. Evitare l'inclusione di un host che fa parte di un orchestrator cluster in un gruppo host. Le progettazioni di contenuto non possono indirizzare un host tramite il relativo indirizzo IP o il nome di dominio completo (FQDN).

È possibile definire più gruppi host sullo stesso agente. Un determinato agente può avere un gruppo host per varianti di un sistema operativo Windows e un altro gruppo host per varianti di un sistema operativo UNIX.

È possibile definire lo stesso gruppo host su uno o più agenti. Quando lo stesso gruppo host si trova su più agenti, l'agente selezionato per l'esecuzione dell'operatore dipende dalla priorità dell'agente.

Per eseguire operatori CA Process Automation su un host remoto, un host locale con un agente CA Process Automation mappato su un gruppo host deve accedere all'host di destinazione. L'agente utilizza SSH per accedere a un host remoto di destinazione e per eseguire operatori su di esso. Definire l'accesso SSH dall'host agente per ogni host di destinazione rappresentato dal gruppo host con un account utente SSH e, facoltativamente, una relazione SSH di trust.

Le proprietà per un gruppo host includono un'impostazione per il numero massimo di connessioni SSH. In genere, le configurazioni predefinite dei server SSHD presentano dei limiti. La connessione SSH rimane aperta mentre il programma o script è in esecuzione sull'host di destinazione. CA Process Automation implementa l'accodamento interno, in base alla destinazione. Se il valore impostato è pari a 20 e si procede all'esecuzione simultanea di 40 script sullo stesso host di destinazione, solo 20 script vengono eseguiti. L'esecuzione dei nuovi script viene avviata al completamento degli altri. Con i gruppi host, in cui lo stesso agente funge da proxy per più host remoti, ciascun host remoto ha un limite specifico. In tal modo, questa impostazione non influisce sul numero di host inclusi nel gruppo host. Il limite del numero di host corrisponde al numero massimo di connessioni TCP simultanee supportate dal sistema operativo per l'agente. Alcuni sistemi operativi supportano un numero elevato di connessioni TCP correnti.

**Importante.** Anche se un gruppo host può includere host remoti con agenti, non creare un gruppo host di host con agenti come mezzo per consentire un riferimento diretto ad essi. Un riferimento tramite touchpoint e touchpoint proxy è altamente preferibile per via della flessibilità e della velocità di elaborazione che esso garantisce.

# Processo di implementazione di gruppo host

È possibile configurare un gruppo host su qualsiasi agente esistente. Un agente non deve essere configurato come touchpoint per ospitare un gruppo host. L'host agente del gruppo host utilizza SSH per accedere ed eseguire azioni su un host remoto. La preparazione di un gruppo host comprende l'abilitazione dell'autenticazione SSH. Quando i responsabili di progettazione dei contenuti utilizzano come destinazione un membro di un gruppo host nella definizione di un operatore, fanno riferimento all'host di destinazione utilizzando il relativo indirizzo IP o FQDN.

La preparazione all'utilizzo di un gruppo host comprende l'esecuzione delle attività e procedure di seguito descritte. Questa panoramica del processo è seguita dagli argomenti che descrivono i dettagli delle procedure.

1. Creazione di un gruppo host (a pagina 256).
2. Configurazione delle proprietà del gruppo host (a pagina 257). Ovvero, specificare i valori per tutte le impostazioni, ad eccezione di Percorso chiavi SSH.
   - Per informazioni sull'immissione dei modelli, consultare Definizione dei modelli di nomi host remoti tramite espressioni regolari (a pagina 259).
   - (Facoltativo) Per l'autenticazione tramite chiave pubblica, configurare Percorso chiavi SSH.

     **Nota:** CA Process Automation ottiene l'accesso con autenticazione tramite chiave pubblica solo quando l'accesso non riesce con le credenziali dell'account utente.
3. Dall'host agente per il gruppo host, verificare che sia installata la versione di Java Virtual Machine (JVM) 1.7 o 1.6 (non oltre la versione 1.6.0_45). JVM comprende JRE o JDK. Sono supportate entrambe le versioni di JVM a 32 e a 64 bit per gli agenti installati sugli host con sistemi operativi Windows. Utilizzare il comando seguente per verificare che la propria versione Java sia valida. Un esempio è indicato di seguito:

   ```
   java -version
   ```

   Esempio di risposta:

   ```
   Versione Java "1.6.0_x", una versione valida
   ```
4. Creazione delle credenziali SSH su host in un gruppo host (a pagina 262). Definire un account utente con le credenziali SSH specificate nelle proprietà del gruppo host per Nome utente remoto e Password remota.
5. Da ciascun host UNIX remoto cui fa riferimento il gruppo host, verificare che la shell Korn sia installata. Se la shell Korn non è stata installata, eseguire una delle azioni seguenti:
   - Installare la shell Korn.
   - Creare un collegamento simbolico da una shell Bash esistente alla shell Korn utilizzando il percorso restituito. Ad esempio:

```
ln –s  /bin/bash /bin/ksh
```

6. Eseguire le operazioni seguenti per completare la configurazione per l'autenticazione della chiave pubblica. Queste operazioni si applicano al Percorso chiavi SSH specificato.

   - Verificare che il percorso immesso come Percorso chiavi SSH nella configurazione del gruppo host esista sull'host agente. In caso contrario, creare il percorso. Ad esempio:

     **Windows:** C:\PAM\Sshkeys

     **UNIX:** /home/PAM/Sshkeys

   - Assicurarsi di disporre dell'utilità ssh-keygen. In caso contrario, scaricarla. In un sistema Windows, ssh-keygen.exe viene visualizzato nella directory C:\Programmi\OpenSSH\bin. La directory bin contiene anche altri file che consentono di utilizzare i comandi UNIX.

     Utilizzare questa utilità per generare la coppia di chiavi pubblica/privata.

   - Verificare che sia possibile copiare un file da un host a un altro. Se necessario, scaricare una utilità di copia, ad esempio SCP o WinSCP.

     Copiare la chiave pubblica dall'host agente in ciascun host remoto.

   - Creare la directory di destinazione e il file di destinazione per la chiave pubblica (a pagina 263).

   - Creazione di una relazione di trust per un host remoto a cui fa riferimento un gruppo host. (a pagina 264)

     **Importante.** Attenersi alle istruzioni riportate di seguito. I passaggi includono requisiti specifici di CA Process Automation diversi dall'implementazione standard di coppie di chiavi DSA.

**Ulteriori informazioni:**

Requisiti specifici di CA Process Automation per la connettività SSH (a pagina 247)

## Creazione di un gruppo host

È possibile aggiungere un gruppo host a un ambiente selezionato e selezionare l'agente. Oppure, è possibile configurare un gruppo host su un agente e selezionare l'ambiente. La combinazione del nome dell'agente e del nome del gruppo host deve essere univoca all'interno di un ambiente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Selezionare l'ambiente da configurare, quindi fare clic su Blocca.

3. Per aggiungere un gruppo host a un ambiente selezionato, completare i passaggi seguenti:

   a. Fare clic con il pulsante destro del mouse sull'ambiente bloccato, quindi selezionare Aggiungi gruppo host.

      Viene visualizzata la finestra di dialogo Aggiungi gruppo host: *ambiente*.

   b. Immettere il nome del gruppo host.

   c. Selezionare un agente visualizzato, quindi fare clic su Aggiungi.

4. Per aggiungere un gruppo host a un agente selezionato, completare i passaggi seguenti:

   a. Espandere il nodo Agenti.

   b. Fare clic con il pulsante destro del mouse sull'agente desiderato, selezionare Configura gruppo host su e selezionare l'ambiente desiderato.

      Viene visualizzata la finestra di dialogo Aggiungi gruppo host agente.

   c. Immettere il nome del gruppo host nel campo Nome del gruppo host e fare clic su OK.

      Se si specifica il nome di un gruppo host esistente, l'agente selezionato viene mappato su quel gruppo host.

5. Visualizzare il nome del gruppo host come segue:

   - Espandere il nodo Tutti i gruppi host per l'ambiente in cui è stato creato il gruppo host.
   - Espandere Agenti e selezionare l'agente con il gruppo host. Il nuovo gruppo host viene elencato nella scheda Touchpoint e Gruppi host associati insieme al percorso della gerarchia di dominio.

**Ulteriori informazioni:**

Processo di implementazione di gruppo host (a pagina 255)

## Configurazione delle proprietà del gruppo host

Dalla scheda Configurazione, è possibile configurare le proprietà di un gruppo host. Si stabilisce la connettività tra l'agente e ciascun host remoto nel gruppo host con prodotti di terze parti.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere il Dominio.
3. Espandere l'ambiente con il gruppo host.

4. Espandere Tutti i gruppi host.

5. Selezionare il gruppo host da configurare e fare clic sulla scheda Proprietà.

6. Impostare le proprietà del gruppo host selezionato.

   a. Impostare Ripristino automatico operatori e Protezione touchpoint come richiesto o accettare il valore predefinito, Eredita dall'ambiente.

   b. Per Percorso chiavi SSH, indicare il percorso di destinazione creato sull'agente per archiviare il file di chiave privata.

      Se l'host agente utilizza un sistema operativo Windows, immettere:
      `C:\PAM\SshKeys`

      Se l'host agente utilizza un sistema operativo UNIX o Linux, immettere:
      `/home/PAM/Sshkeys`

      **Importante.** Creare il percorso di destinazione sull'host agente.

   c. Per ciascun modello di nome host remoto, fare clic sul pulsante Aggiungi parametro e definire un modello di nome host.

      Consultare Definizione dei modelli di nome host remoto tramite espressioni regolari (a pagina 259).

   d. Immettere le credenziali dell'account utente che è stato creato o che si intende creare su ciascun host remoto a cui il gruppo host fa riferimento.

      **Nota:** Se si configura l'autenticazione tramite chiave pubblica, il valore deve essere specificato come *nome utente* nel comando per generare i file delle chiavi. Se si utilizza l'autenticazione tramite chiave pubblica con una passphrase, immettere la passphrase per la password remota.

   e. Completare i campi intuitivi rimanenti.

7. Fare clic su Salva.

8. Fare clic con il pulsante destro del mouse sull'ambiente bloccato, quindi selezionare Sblocca.

   La configurazione delle proprietà è parte della configurazione totale. È necessario creare un account utente su ciascun host remoto con le credenziali configurate qui. Ciò fornisce l'accesso SSH dall'agente a ciascun host remoto nel gruppo host. Stabilire una relazione di trust con chiavi pubbliche e private è facoltativo.

**Ulteriori informazioni:**

Processo di implementazione di gruppo host (a pagina 255)

## Modalità di definizione dei modelli di nomi host remoto tramite espressioni regolari

Quando si configurano gruppi host, si specificano i modelli di nome host e di indirizzo IP o entrambi. Gli operatori di espressione regolare che è possibile applicare durante la definizione di modelli di host remoto per gruppi host sono i seguenti:

- ^ (punto di inserimento) indica che inizia con.
- \ (Esc) indica l'interpretazione del carattere dell'operatore immediatamente successivo come valore letterale.
- . (punto) all'interno di un'espressione indica qualsiasi carattere. L'espressione a.b corrisponde a qualsiasi stringa di tre caratteri che inizia con "a" e termina con "b".
- .* (punto asterisco), indica l'accettazione di qualsiasi carattere un numero qualsiasi di volte. L'espressione a.*b corrisponde a una stringa di qualsiasi lunghezza che inizia con "a" e termina con "b".
- $ (segno di dollaro) significa termina con.

Considerare l'espressione regolare come un modo per esprimere qualcosa nel nome di dominio completo (FQDN), ad esempio:

- un modello di avvio (^String)
- un modello centrale (String)
- un modello finale (String$)
- un modello preciso (^StringWithEscapedDots$)

La seguente tabella contiene esempi che consentono di immettere modelli di nome host in modo da garantire un'elaborazione efficiente. Se si specifica un nome di dominio completo (FQDN) o sottodominio senza operatori, il nome di dominio completo (FQDN) o un gruppo che si intende mappare viene trovato, ma l'elaborazione non è efficiente. Una procedura ottimale include le seguenti combinazioni di espressioni regolari nei modelli di nomi host immessi per i modelli di host remoto.

| Combinazioni comuni | Descrizione | Esempio di nome di dominio completo (FQDN) ed esempio di gruppo host |
|---|---|---|
| ^ <hostname> | Il punto di inserimento come primo carattere indica che il modello inizia con il testo che segue il punto di inserimento. | **FQDN:** ^host1\.ca\.com$ corrisponde solo a host1.ca.com<br>(ma, host1\.ca\.com $ senza il punto di inserimento cerca ogni host con un nome che termina con host1.ca.com, ad esempio aaaahost1.ca.com)<br>**Gruppo:**<br>ca\.com $ senza il punto di inserimento corrisponde a ogni nome completo di dominio (FQDN) nel sottodominio ca.com. |

| Combinazioni comuni | Descrizione | Esempio di nome di dominio completo (FQDN) ed esempio di gruppo host |
|---|---|---|
| \. | La combinazione di escape punto (\.) indica che il punto viene interpretato come valore letterale. | **FQDN:** ^host1\.ca\.com$ corrisponde solo a host1.ca.com<br>(ma, ^ host.ca.com$ senza escape prima di ogni punto può corrispondere a:<br>host1Mca0com)<br>**Group:** ^ host.\.ca\.com$ con un punto dopo l'host può corrispondere a un host denominato {host0, host1,... hostZ} nel dominio ca.com. |
| .*<dominio> | La combinazione di punto asterisco (.*) può corrispondere a ogni cosa. | **Group:** .*\.ca\.com$, un dominio preceduto da .* corrisponde a tutti gli host nel dominio. |
| <domain name>$ | Il segno di dollaro dopo un nome di dominio indica che il modello termina con il dominio specificato. | **FQDN:** ^host1\.ca\.com$ corrisponde solo a host1.ca.com<br>(ma ^host1\.ca\.com senza l'operatore $ finale può corrispondere a:<br>host1.ca.comaaaaaaa) |

### Esempi

**Modelli di indirizzo IP remoto**

Specifica qualsiasi combinazione di quanto segue, in cui gli indirizzi IP sono statici piuttosto che dinamici. Fare clic su Aggiungi per creare ciascuna riga.

- Un elenco di indirizzi IP IPv4.
- Una o più subnet IPv4 mediante notazione CIDR.

**Modelli del nome host remoto**

Specifica un gruppo di host remoti con un elenco di nomi di dominio completi (FQDN) o di modelli di espressioni regolari per un sottodominio. Selezionare Aggiungi per creare una riga per ciascuna voce di modello.

Ad esempio:

- abc\.nomeazienda\.com
- .*pam-lnx\.nomeazienda\.com$

  Questo modello corrisponde a qualsiasi nome host che termina in pam-lnx nel dominio dell'azienda, in cui "nomeazienda" viene sostituito dal nome dell'azienda.

- ^computer1\.nomeazienda\.com$

  In particolare, ^computer1\.nomeazienda\.com$ esprime un nome di dominio completo (FQDN) come espressione regolare. Questo modello corrisponde solo al FQDN che soddisfa tutti i criteri seguenti:

  inizia con *computer1.*

  finisce con *com.*

  contiene *computer1*, *punto*, *nomeazienda*, *punto* e infine *com*.

## Creazione delle credenziali SSH su host in un gruppo host

Una configurazione di gruppo host specifica le credenziali SSH come indicato di seguito.

- Nome utente remoto
- Password remota

Accedere a ciascun host a cui fa riferimento il gruppo host. Creare un account utente con queste credenziali SSH. L'account utente SSH deve disporre di autorizzazioni sufficienti per le attività seguenti:

- Per eseguire attività amministrative.
- Per eseguire gli operatori di CA Process Automation su ciascun computer di destinazione.

L'agente utilizza il nome utente dell'account utente SSH per connettersi al daemon SSH nell'host remoto di destinazione. L'host di destinazione può essere qualsiasi host che corrisponda ai modelli di nome host remoto o di indirizzo IP remoto nella configurazione del gruppo host.

L'host agente del gruppo host avvia una connessione all'host remoto come indicato di seguito:

1. Accede all'host remoto con le credenziali specificate.
2. Crea una directory temporanea chiamata c2otmp.

   Questa directory viene creata nella directory /home dell'utente SSH se l'host di destinazione è un computer UNIX. Ad esempio:

   ```
   /home/<user_name>/c20tmp
   ```

**Ulteriori informazioni:**

Processo di implementazione di gruppo host (a pagina 255)

## Creazione della directory di destinazione e del file di destinazione per la chiave pubblica.

Se si decide di creare la relazione di trust facoltativa agli host remoti a cui fa riferimento il gruppo host, verificare l'esistenza della directory e del file seguenti su ogni host remoto. Se il file o la directory non esistono, crearli.

Quanto segue è necessario su ogni host remoto prima di creare la relazione di trust dall'host con il gruppo host.

- La directory .ssh in /home/<user_name>, la directory di destinazione per <user_name>.pub
- Un file authorized_keys, a cui la chiave pubblica contenuta in <user_name> .pub può essere aggiunta. Il file ~/.ssh/authorized_keys è il file predefinito che elenca le chiavi pubbliche consentite per l'autenticazione DSA.

Per creare la directory .ssh e il file authorized_keys su un host remoto UNIX o Linux

**Attenersi alla procedura seguente:**

1. Utilizzare ssh per accedere a un host remoto con il nome utente remoto e la password remota configurati per il gruppo host.
2. Verificare che la directory corrente sia la directory principale. Immettere:

   pwd

   La risposta è:

   /home/*user_name*
3. Creare la directory .ssh in questo percorso e accedere alla nuova directory.

   ```
   mkdir .ssh
   CD .ssh
   ```
4. Creare authorized_keys nella directory .ssh.

   ```
   cat > authorized_keys
   ```

   Un file authorized_keys vuoto viene creato nella directory /home/*user_name*/.ssh.

**Per creare la directory .ssh e il file authorized_keys su un host remoto Windows**

1. Utilizzare il desktop remoto per accedere all'host remoto con il nome utente remoto e la password remota configurati per il gruppo host.
2. Accedere alla cartella principale. Ad esempio, \Users*user_name.*
3. Se una cartella .ssh non esiste, creare una nuova cartella e denominarla .ssh.
4. Nella seguente cartella, creare un file denominato authorized_keys privo di estensione.

   \Users*user_name*\.ssh

Il seguente file vuoto è stato creato.

\Users*user_name*\.ssh\authorized_keys

## Creazione di una relazione di trust per un host remoto a cui fa riferimento un gruppo host

Un *host remoto* è un host a cui fa riferimento un gruppo host. Il gruppo host è configurato su un host con un agente. Generalmente l'host remoto non dispone di alcun agente. Per uilizzare come destinazione un host remoto è necesario che un operatore del processo disponga della connettività SSH tra un host agente e l'host remoto di riferimento.

Stabilire una connessione SSH utilizzando uno dei metodi seguenti:

- Creare una relazione di trust tra l'host agente e l'host remoto. Questo metodo crea una coppia di chiavi pubblica/privata.
- Creare un account utente sull'host remoto. Questo metodo crea le credenziali.

Quando si creano un account utente *e* una relazione di trust, il prodotto utilizza la relazione di trust come meccanismo di backup. Se l'autenticazione non avviene correttamente per le credenziali configurate, il prodotto esegue l'autenticazione con la coppia di chiavi.

Generare una coppia di chiavi con il programma SSH-keygen. Salvare la chiave privata nel percorso chiavi SSH configurato, quindi copiare la chiave pubblica in ciascun host remoto a cui fa riferimento il gruppo host. Collocare il file di chiave pubblica in una posizione individuabile dal daemon SSH. Il daemon OpenSSH, sshd, cerca la chiave in /home/*user_name*/.ssh/authorized_keys.

È possibile creare una relazione di trust per un host remoto a cui fa riferimento un gruppo host.

**Attenersi alla procedura seguente:**

1. Accedere all'host che contiene l'agente in cui è definito il gruppo host.
2. Aprire un prompt dei comandi e modificare le directory con un percorso da cui generare la coppia di chiavi.

   Ad esempio, se OpenSSH è stato scaricato in un sistema Windows, modificare la directory in C:\Program Files\OpenSSH\bin contenente il programma ssh-keygen.

3. Generare una coppia di chiavi con il comando seguente:

   ```
   ssh-keygen -t dsa -b 1024 -f user_name
   ```

   ***user_name***

   Definisce il valore configurato come Nome utente remoto nel gruppo host.

   Il messaggio e il prompt seguenti vengono visualizzati:

   ```
   Generare la coppia di chiavi dsa pubblica/privata.
   Immettere la passphrase <empty for no passphrase>:
   ```

4. Immettere il valore configurato come Password remota nel gruppo host. Questo valore è obbligatorio.

   Viene visualizzato il prompt seguente:

   ```
   Immettere la stessa passphrase:
   ```

5. Immettere di nuovo il valore della password remota.

   Vengono visualizzati i messaggi seguenti:

   ```
   L'identificazione è stata salvata in user_name.
   Il file della chiave pubblica è stato salvato in user_name.pub.
   L'impronta digitale della chiave è:
       fingerprint_string login_name@host_name
   ```

   Il prodotto crea il file di chiave privata denominato *user_name* e il file di chiave pubblica denominato *user_name*.pub. La passphrase per il file di chiave è uguale alla password dell'account utente utilizzato per l'accesso SSH.

6. Spostare il file di chiave privata denominato *user_name* nella posizione configurata come Percorso chiavi SSH nel gruppo host. Ad esempio:

   - **Windows:** C:\PAM\Sshkeys
   - **UNIX:** /home/PAM/Sshkeys

7. Trasferire il file di chiave pubblica (*user_name*.pub) su ogni host a cui fa riferimento il gruppo host e spostarlo in una posizione individuabile dal daemon SSH.

   Daemon SSH differenti seguono convenzioni diverse. Esaminare le opzioni ssh-keygen per i requisiti di formattazione del file di chiave pubblica.

8. Per OpenSSH, aggiungere la chiave pubblica da *user_name*.pub al file che contiene tutte le chiavi autorizzate impiegate dall'host. Il daemon OpenSSH (sshd) cerca il file authorized_keys. Il file authorized_keys deve trovarsi nella directory .ssh, nel percorso della directory principale.

   a. Eseguire il seguente comando su ogni host a cui fa riferimento il gruppo host:

      ```
      cat user_name.pub >> home/user_name/.ssh/authorized_keys
      ```

   b. Portare gli utenti alla directory principale e riavviare il servizio ssh:

      ```
      directory principale
      ```

      ```
      riavvio del servizio sshd
      ```

9. Verificare che l'accesso sia stabilito. Accedere all'host con l'agente e all'ssh all'host remoto. Se l'accesso riesce, la relazione di trust è stabilita. Immettere il comando seguente dall'host agente:

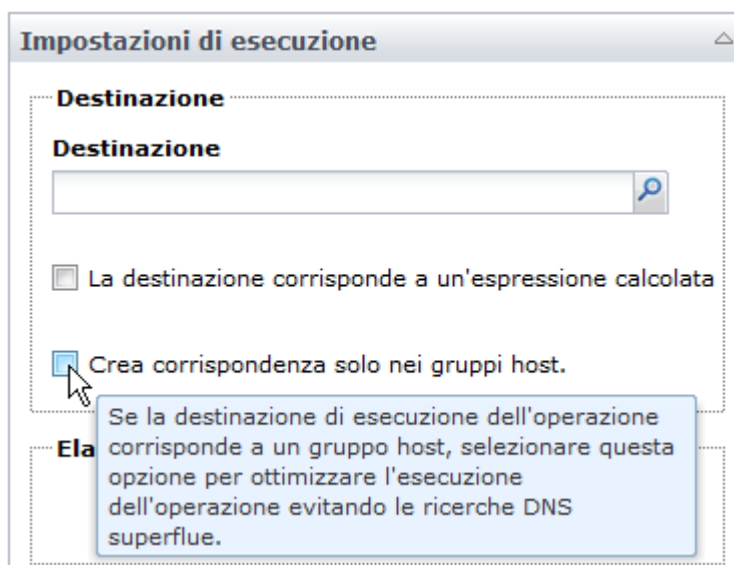
   ```
   ssh user_name@remote_host
   ```

**Ulteriori informazioni:**

Processo di implementazione di gruppo host (a pagina 255)
Requisiti specifici di CA Process Automation per la connettività SSH (a pagina 247)

# Procedura per garantire un'elaborazione efficiente dei riferimenti del gruppo host

Questo argomento, che riguarda i responsabili di progettazione dei contenuti, è utile per l'amministratore a titolo informativo.

Durante la progettazione di un processo, i responsabili di progettazione dei contenuti specificano le impostazioni di esecuzione per ciascun operatore. L'esempio seguente mostra una finestra di dialogo parziale con il campo Destinazione e la casella di controllo Crea corrispondenza solo nei gruppi host.

Se il campo Destinazione contiene un nome di touchpoint, un nome di touchpoint proxy o un ID agente, deselezionare la casella di controllo Crea corrispondenza solo nei gruppi host.

Se il campo Destinazione contiene un indirizzo IP di un host specifico, selezionare la casella di controllo Crea corrispondenza solo nei gruppi host. L'inserimento di un indirizzo IP o un nome host nel campo Destinazione è valido solo se un gruppo host nell'ambiente attuale fa riferimento all'host corrispondente.

**Importante.** Se un processo è destinato all'esportazione in una cartella come pacchetto di contenuto, non immettere un indirizzo IP nel campo Destinazione. Immettere invece un nome di set di dati contenente l'indirizzo IP. Altrimenti:

- Selezionare La destinazione corrisponde a un'espressione calcolata.
- Selezionare Crea corrispondenza solo nei gruppi host. Un set di dati che fa riferimento a un indirizzo IP è valido se un gruppo host nell'ambiente attuale fa riferimento all'host corrispondente.

Per comprendere lo scopo della casella di controllo, considerare il caso in cui:

- Il campo Destinazione contiene la voce *some_host,* in cui la voce è il nome di un host in un gruppo host.
- La casella di controllo Crea corrispondenza solo nei gruppi host è deselezionata.

L'elaborazione di runtime valuta ed elabora la voce Destinazione nella sequenza seguente:

1. Se la voce è un nome di touchpoint, viene eseguita sull'host con l'agente associato al touchpoint.
2. Se la voce è un nome di touchpoint proxy, viene eseguita sull'host con connessione SSH all'agente associato al touchpoint proxy.
3. Se la voce è un ID agente, viene eseguita sull'host con questo ID agente.
4. Se la voce è un indirizzo IP o un nome host cui fa riferimento un gruppo host, viene eseguita su quell'host.

   **Nota:** l'operatore restituisce un errore se si seleziona la casella di controllo Crea corrispondenza solo nei gruppi host quando la destinazione specificata *non* è compresa in un gruppo host. L'operatore restituisce un errore anche se la destinazione è un nome di touchpoint, un nome di touchpoint proxy o un ID agente valido.

# Casi in cui evitare l'utilizzo dei riferimenti di gruppo host come destinazioni

Quando un processo viene esportato in una cartella come pacchetto di contenuto:

- *Non è possibile* modificare i processi nell'ambiente di importazione.
- *È possibile* modificare i set di dati nell'ambiente di importazione.

Se il campo Destinazione di un operatore contiene un indirizzo IP o un nome host, non è possibile la corretta esecuzione del processo importato. Non è possibile modificare la voce Destinazione di un operatore nell'ambiente di importazione.

Per i contenuti ridistribuibili si consiglia di utilizzare set di dati per i parametri di configurazione. Il responsabile di progettazione dei contenuti crea una variabile del set di dati per l'archiviazione di un indirizzo IP. In seguito, il responsabile di progettazione dei contenuti immette quella variabile del set di dati nel campo Destinazione per l'operatore. Un amministratore nell'ambiente di importazione può aggiornare il set di dati con un valore di indirizzo IP cui fa riferimento un gruppo host nell'ambiente di importazione.

# Differenze tra gruppi host e touchpoint proxy

I gruppi host e touchpoint proxy sono simili nei seguenti aspetti:

- Entrambi operano sugli agenti.
- Entrambi accedono a host remoti tramite SSH.
- Entrambi supportano gli stessi operatori di CA Process Automation che possono essere eseguiti sull'host remoto tramite SSH.
- Le categorie configurate per gli operatori richiesti devono essere eseguite sull'host agente in cui è configurato il touchpoint proxy o il gruppo host.

I gruppi host differiscono dai touchpoint proxy nei seguenti aspetti:

- Il rapporto tra un gruppo host e potenziali host di destinazione è di uno a molti, mentre il rapporto tra un touchpoint proxy e l'host di destinazione è di uno a uno.
- I responsabili di progettazione dei contenuti possono utilizzare come destinazione più host con touchpoint proxy associati specificando un gruppo touchpoint. I responsabili di progettazione dei contenuti non possono utilizzare come destinazione più host che dispongano di un solo gruppo host di riferimento.
- I responsabili di progettazione dei contenuti specificano un host remoto come destinazione tramite il relativo nome di touchpoint quando l'host remoto dispone di un touchpoint proxy associato. I responsabili di progettazione dei contenuti specificano un host remoto come destinazione tramite l'indirizzo IP o il nome di dominio completo (FQDN) quando l'host remoto ha un gruppo host di riferimento.

# Capitolo 12: Amministrazione delle categorie di operatore e dei gruppi di operatori personalizzati

Questo capitolo descrive i concetti e le procedure attinenti alla configurazione delle impostazioni predefinite comuni per gli operatori a livello di categoria. Inoltre illustra i valori di configurazione per le variabili che è possibile definire per i gruppi di operatori personalizzati.

**Nota:** non è necessario configurare i moduli (categorie di operatore). Come procedura ottimale, si consiglia al responsabile di progettazione dei contenuti di creare set di dati globali per le impostazioni di modulo. Il responsabile di progettazione dei contenuti utilizza quindi le espressioni che fanno riferimento alle variabili del set di dati nelle proprietà dell'operatore.

Questa sezione contiene i seguenti argomenti:

# Categorie dell'operatore e cartelle dell'operatore

Le categorie dell'operatore corrispondono alle cartelle dell'operatore. Gli amministratori configurano le categorie dell'operatore nella scheda Moduli, a partire dal livello di dominio. I responsabili di progettazione dei contenuti espandono le cartelle dell'operatore per visualizzare un gruppo di operatori nella categoria denominata. Nel riquadro Operatori della scheda Progettazione sono visualizzate le cartelle Operatore.

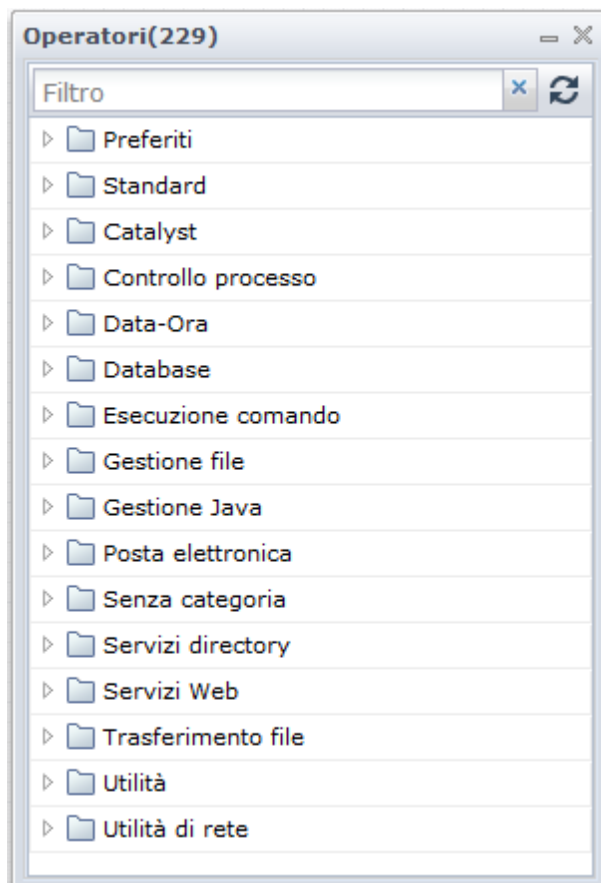
Fare clic sulla scheda Configurazione, selezionare Dominio, quindi fare clic sulla scheda Moduli per elencare le categorie dell'operatore in Nome.

**Nota:** l'elenco Nome può includere anche i gruppi pubblicati creati per gli operatori personalizzati. I responsabili di progettazione dei contenuti possono espandere le cartelle di gruppo per visualizzare un gruppo di operatori personalizzati nel gruppo di configurazione denominato. Le cartelle del gruppo di configurazione visualizzate per gli operatori personalizzati sono riportate anche nel riquadro Operatori della scheda Progettazione.

Contenuti di "Dominio"

Protezione | Proprietà | Moduli | Trigger | Audit trail

| Nome | Descrizione |
|---|---|
| Catalyst | Fornisce l'accesso ai connettori Catalyst. |
| Controllo processo | Esegue, monitora e controlla i processi di CA Process Automation. |
| Data-Ora | Esegue i vincoli data/ora nei processi di CA Process Automation. |
| Database | Modulo di database per la comunicazione con i server di database. |
| Esecuzione comando | Esegue i programmi e gli script su sistemi operativi host. |
| Gestione file | Il modulo monitora le directory, i file e il loro contenuto. |
| Gestione Java | Fornisce al sistema esterno un'interfaccia di gestione con supporto JMX. |
| Posta elettronica | Servizio di posta elettronica che legge i messaggi dal server mediante i protocolli IMAP o POP3. |
| Servizi directory | Fornisce un'interfaccia per il supporto LDAP/AD. |
| Servizi Web | Fornisce un'interfaccia ai servizi esterni visualizzati mediante SOAP. |
| Trasferimento file | Fornisce operazioni di trasferimento file (FTP/SFTP). |
| Utilità | Il modulo contiene operatori di utilità utilizzati nei processi PAM |
| Utilità di rete | Fornisce utilità e operazioni ai servizi di rete. |

Fare clic sulla scheda Progettazione, quindi su Visualizza e selezionare Operatori per visualizzare i nomi di cartella con lo stesso raggruppamento di operatori delle categorie di operatore configurate.

I responsabili di progettazione dei contenuti selezionano gli operatori dal riquadro Operatori per creare processi automatizzati. Ciascun operatore esegue un'operazione specifica. Affinché i responsabili di progettazione possano individuare velocemente l'operatore adeguato, CA Process Automation raggruppa gli operatori in categorie di uso comune. Ad esempio, tutti gli operatori che vengono utilizzati per il trasferimento file mediante FTP vengono raggruppati in una cartella denominata Trasferimento file.

I valori della categoria di operatore si configurano a livello di dominio. I valori vengono ereditati a livello di ambiente, quindi a livello di orchestrator o di touchpoint agente. È possibile sostituire i valori ereditati a qualsiasi livello. Gli operatori ereditano quindi i valori predefiniti della categoria di operatore. I responsabili di progettazione dei contenuti possono accettare o sovrascrivere questi valori.

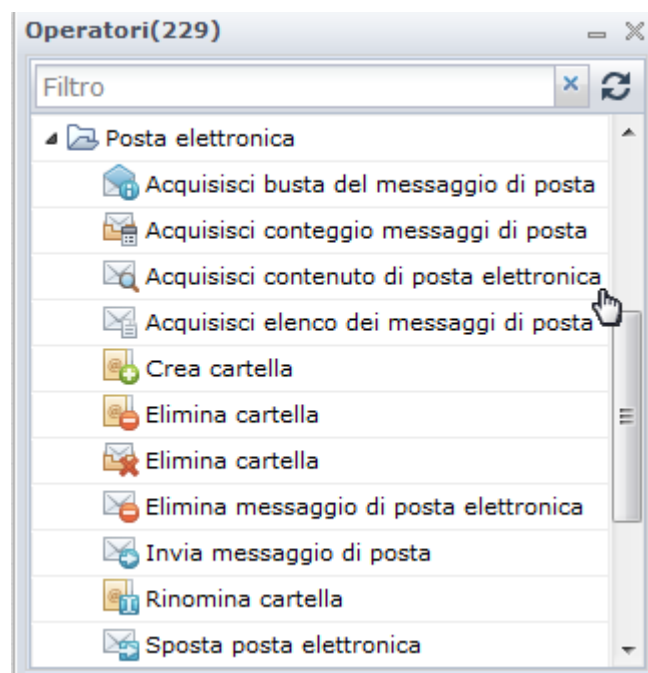
**Ulteriori informazioni:**

Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)

# Esempio: Impostazioni di categoria utilizzate dall'operatore

Durante la configurazione delle impostazioni a livello di dominio per ciascuna categoria nella scheda Moduli, tenere in considerazione i valori utilizzati normalmente dagli operatori. Se le impostazioni vengono configurate in base ai valori più frequenti, la configurazione a livelli inferiori verrà eseguita solo per le eccezioni.

Considerare la configurazione di Proprietà messaggio di posta elettronica, in cui il valore Protocollo predefinito per la connessione è impostato su IMAP e il campo Porta predefinita del server di posta è impostato su 143. Configurare il server di posta predefinito e la password predefinita.

Quando un responsabile di progettazione dei contenuti automatizza un processo per i messaggi di posta elettronica, uno degli operatori disponibili per l'uso è Acquisisci contenuto di posta elettronica.

Quando un responsabile di progettazione dei contenuti trascina l'operatore Acquisisci contenuto di posta elettronica all'area di disegno, vengono visualizzate le proprietà di Get_Email_Content_1. Notare la somiglianza tra le proprietà del messaggio di posta elettronica, configurate sulla scheda Moduli nella scheda Configurazione e i parametri di accesso al server di posta elettronica per le proprietà di Get_Email_Content_1, visualizzate nella scheda Progettazione.

| L'operatore Acquisisci contenuto di posta elettronica eredita i valori per questi parametri di accesso al server di posta elettronica | da valori configurati nell'impostazione del modulo Posta elettronica per Proprietà messaggio di posta elettronica |
|---|---|
| Protocollo di connessione | Protocollo predefinito per la connessione |
| Host del server di posta | Host del server di posta predefinito |
| Porta del server di posta | Porta predefinita del server di posta |
| Nome utente | Nome utente predefinito |
| Password | Password predefinita |

Il responsabile di progettazione dei contenuti può configurare i valori specifici del processo e sostituire i valori predefiniti configurati in precedenza. Oppure, il responsabile di progettazione dei contenuti può lasciare il campo vuoto per ereditare i valori predefiniti. In questo esempio, un protocollo di connessione vuoto utilizza IMAP e una porta del server di posta vuota utilizza la porta 143.

# Configurazione delle categorie operatore

Gli amministratori in grado di bloccare il dominio possono configurare o modificare le impostazioni predefinite per le categorie di operatore a livello di dominio. Queste configurazioni vengono ereditate. È possibile modificare queste impostazioni a livello di ambiente, orchestrator e agente. Per ulteriori informazioni, consultare la sezione Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318).

È possibile sostituire i valori predefiniti per tutti i campi di categoria di operatore a livello di operatore. I valori immessi per le categorie di operatore sono tutti predefiniti. Quando un operatore viene configurato con un campo vuoto, tale operatore eredita il valore predefinito del campo corrispondente dall'impostazione della categoria. Quando si seleziona un valore nella scheda Modulo, niente viene abilitato o disabilitato. È possibile specificare tutti i valori predefiniti, a propria discrezione. Quando si configurano queste stesse opzioni a livello di operatore, la selezione di un'opzione disabilita le altre.

**Nota:** per ulteriori informazioni, consultare la G*uida di riferimento per la progettazione dei contenuti* per la configurazione dell'operatore di questi stessi campi.

Per espandere un campo per una voce più lunga dello spazio fornito, fare clic con il tasto destro del mouse sul campo e selezionare Espandi. Si apre una finestra di dialogo con una casella di testo.

## Informazioni su Catalyst

Catalyst viene configurato con le impostazioni seguenti:

- Impostazioni Proprietà Catalyst.
- Impostazioni Protezione Catalyst.

Il modello servizi unificato (Unified Service Model, USM) è uno schema di tipi di oggetto e proprietà comuni in cui vengono convertiti i dati da tutti i connettori. Lo schema USM abilita l'analisi dei dati da tutti i gestori di dominio. È possibile analizzare i dati in un'interfaccia comune con formattazione identica nei gestori di dominio.

Gli operatori Catalyst consentono di utilizzare i connettori Catalyst in processi automatizzati. Gli operatori Catalyst supportano le interfacce seguenti:

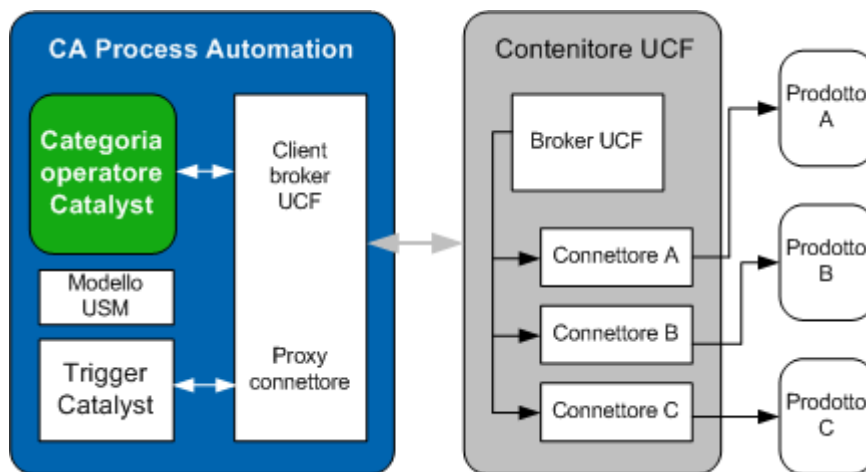
- Creazione, lettura, aggiornamento, eliminazione (CRUD)
- Esegui
- Sottoscrizione a eventi

Gli operatori presentano tipi di oggetto e proprietà USM.

Il modello USM comune e le interfacce UCF standard consentono la compatibilità di Catalyst con tutti i contenitori e connettori UCF.

CA Process Automation integra i componenti UCF-USM seguenti:

- Categoria operatore Catalyst
- Trigger Catalyst

Le categorie di operatore Catalyst e Trigger Catalyst sono client di connettori UCF remoti che utilizzano le interfacce proxy del broker UCF e del connettore, come illustrato di seguito:

## Configurazione delle impostazioni predefinite di Catalyst

È possibile configurare le impostazioni predefinite di Catalyst completando le schede seguenti:

- Proprietà predefinite di Catalyst
- Protezione Catalyst predefinita
- Attestazioni Catalyst predefinite
- Attestazioni password Catalyst predefinite

**Nota:** I valori di password sono crittografati.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Catalyst e selezionare Modifica.

   Viene visualizzata la scheda Proprietà predefinite di Catalyst.

3. Configurare le proprietà predefinite di Catalyst.

   a. Inserire l'URL predefinito appropriato nel campo URL del broker UCF. L'operatore associato eredita questa impostazione. Di seguito sono riportati esempi di URL per comunicazione di base e per quella protetta:

      `http://`*`hostname`*`:7000/ucf/BrokerService`

      `https://`*`hostname`*`:7443/ucf/BrokerService`

   b. Inserire il nome appropriato nel campo Nome file di configurazione delle proprietà del prodotto. Questo file viene utilizzato per personalizzare le proprietà visualizzate nell'operatore generico Crea.

4. Fare clic sulla scheda Protezione Catalyst predefinita e immettere l'ID utente e la password predefiniti di Catalyst.

5. Fare clic sulla scheda Attestazioni Catalyst predefinite e completare la configurazione.

   a. Fare clic su Aggiungi parametro e immettere il nome della prima attestazione con il relativo valore.

   b. Ripetere questa fase per ciascuna attestazione predefinita.

   c. Utilizzare le frecce su e giù per ordinare le attestazioni come necessario.

6. Fare clic sulla scheda Attestazioni password Catalyst predefinite e completare la configurazione.

   a. Fare clic su Aggiungi parametro e immettere il nome della prima attestazione con il relativo valore.

   b. Ripetere questa fase per ciascuna attestazione di password predefinita.

   c. Utilizzare le frecce su e giù per ordinare le attestazioni come necessario.

7. Fare clic su Salva e chiudi.

8. Fare clic su Salva.

9. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Catalyst (a pagina 276)
Configurazione delle categorie operatore (a pagina 276)

## Caricamento dei descrittori di Catalyst

Un descrittore del connettore di Catalyst specifica le funzioni del connettore, tra cui le operazioni che supporta. Ciascuna operazione specifica ulteriormente i parametri associati. È possibile caricare i descrittori in CA Process Automation. L'operatore Esegui, un operatore nella categoria operatore Catalyst, utilizza i descrittori. Il prodotto visualizza i descrittori caricati a diversi livelli:

- Categorie operazione (elenco a discesa)
- Operazione (elenco a discesa)
- Parametri (valori editor)

È possibile caricare un descrittore Catalyst dall'host locale nell'orchestrator di dominio remoto come risorsa dell'utente. Il prodotto replica tutte le risorse in ogni nuovo orchestrator.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Espandere Gestisci risorse utente nel riquadro sinistro.
3. Espandere la cartella Repository, espandere la cartella Risorsa utente, quindi selezionare la cartella ucf. If
4. Fare clic su Nuovo.
5. Completare i campi nel riquadro Aggiungi nuova risorsa se necessario.

   **Nota:** Lasciare vuoto il campo Percorso sottocartelle della risorsa. Il passaggio 3 definisce il percorso della sottocartella ucf.
6. Fare clic su Salva.

   L'elenco delle risorse dell'utente visualizza il descrittore.

Risorsa utente : ".c2ouserresources/ucf"

| Nome | Tipo di file | Percorso file | Modulo | Descrizione |
|---|---|---|---|---|
| ucfpamconnector-descriptors | jar | .c2ouserresources/ucf/ucfpamconnector-descriptors.jar | itpamucfconnector | ucfpamconnector-descriptors |

**Nota**: Il descrittore è disponibile nell'operatore Esegui dopo il riavvio dell'orchestrator. Per ulteriori informazioni sull'operatore Esegui nella categoria Catalyst, consultare *Guida di riferimento per la progettazione dei contenuti*.

**Ulteriori informazioni:**

Aggiunta di una risorsa alle Risorse utente (a pagina 342)

# Informazioni su Esecuzione comando

Gli operatori Esecuzione comando consentono di eseguire script di shell o programmi eseguibili su qualsiasi agente o orchestrator. Questa categoria consente l'accesso a dati e risorse alle periferiche di rete che supportano i protocolli di interfaccia Telnet e SSH (Secure Shell).

Di seguito è riportato l'elenco degli operatori:

- Esegui programma
- Esegui script
- Esegui comando SSH
- Esegui script SSH
- Esegui comando Telnet
- Esegui script Telnet

Se si stanno eseguendo script, seguire le convenzioni dei sistemi operativi Windows o UNIX per renderli eseguibili. In CA Process Automation, gli script restituiti risultano come variabili di set di dati di CA Process Automation.

- Per i sistemi UNIX, la prima riga dello script specifica il percorso completo all'interprete desiderato. Ad esempio:

  `#!/bin/sh`

  Specifica l'esecuzione tramite sh, Bourne shell su sistemi quali Oracle Solaris. Su sistemi Linux, questa voce è un collegamento a un altra shell, ad esempio bash. Un operatore di script può eseguire uno script per cui l'host di destinazione dispone di un interprete.

  Includere i comandi shell, come *cp* o *dir*, in un file di script eseguibile.

  `#!/usr/bin/perl`

  Se posizionato nella parte superiore di uno script Perl, indica il server Web in cui si trova l'eseguibile Perl.

- Per i sistemi Windows, l'estensione del nome del file definisce l'interprete di script. Per Windows, definire le associazioni di file per eseguire gli script automaticamente. Sono supportate le estensioni seguenti:

  `*.ps1`

  File PowerShell di Windows.

  `*.exe`

  File eseguibile che installa ed esegue i programmi e le routine.

  `* .cmd`

  File batch composto da una sequenza di comandi; simile a un file .BAT, ma eseguito dal programma CMD.exe anziché dal programma COMMAND.com.

  `* .vbs`

  File VBScript.

  `* .wsh`

  Un file di testo Windows Script Host con parametri per uno script, ad esempio un file .vbs; richiede Microsoft WScript o Microsoft Cscript per aprire il file.

**Ulteriori informazioni:**

Configurazione di Esecuzione comando: Proprietà Telnet predefinite (a pagina 283)

## Configurazione di Esecuzione comando: Proprietà SSH predefinite

Quando si configurano le proprietà SSH predefinite, configurare gli elementi seguenti:

- Le specifiche del tipo di terminale
- I dettagli di autenticazione per accedere a un host remoto
- (Facoltativo) Se cambiare utente dopo l'accesso

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Esecuzione comando e selezionare Modifica.
3. Selezionare la scheda Proprietà SSH predefinite.
4. Selezionare il tipo di pseudoterminale predefinito da richiedere sulla connessione SSH.

   **Nota:** VT100 in genere interagisce con gli host di Linux, VT400 invece interagisce con gli host di Windows.

5. Selezionare la porta predefinita da utilizzare per connettersi all'host remoto.

   **Nota:** La porta 22 è la porta TCP/UDP di sistema per il protocollo SSH (Secure Shell).

6. Immettere il valore predefinito relativo al nome utente da utilizzare per accedere all'host remoto.

7. Specificare i valori predefiniti della chiave privata:

   a. Indicare se utilizzare una chiave privata per l'accesso.

      **Nota:** In alternativa, utilizzare le informazioni di password.

   b. Immettere la password predefinita da utilizzare per accedere all'host remoto.

   c. Fare clic su Sfoglia (...) e recuperare il contenuto della chiave privata, ossia il contenuto di una chiave privata predefinita per l'accesso all'host remoto.

   d. Immettere il percorso di una chiave privata predefinita con cui accedere all'host remoto.

   e. Immettere la passphrase con cui sbloccare il contenuto della chiave privata predefinita.

      **Nota:** la passphrase è richiesta se la chiave privata predefinita è stata creata con una passphrase.

8. Specificare i valori predefiniti per l'esecuzione dello script o dei comandi indicati come un utente diverso.

   a. Indicare se eseguire lo script o i comandi specificati come un altro utente.

   b. Immettere il comando specifico del sistema operativo per cambiare utente sull'host remoto. Il comando "su -root" consente di passare gli utenti all'utente principale. Ad esempio:

      ```
      su - <username>
      ```

      ```
      sudo su - <username>
      ```

   c. Immettere un'espressione regolare per il prompt di testo predefinito se l'host remoto richiede una password per il cambio di utente.

      Il prompt è in genere "Password: " o "password: ". L'espressione regolare ".*assword: " corrisponde a qualsiasi input (incluse nuove righe) e una lettera "P" maiuscola o "p" minuscola seguita da "assword: ".

   d. Immettere la password predefinita nel prompt di testo se l'host remoto richiede una password per il cambio di utente.

e. Immettere un'espressione regolare nel prompt dei comandi per indicare che l'host remoto è pronto per i comandi, ad esempio il cambio di utente.

   I prompt dei comandi standard sono i segni # (cancelletto), > (maggiore) e ? (punto interrogativo). La voce .*[$>?:#] corrisponde a qualsiasi input (incluse le nuove righe) seguito dai segni #, >, ?, $ (simbolo del dollaro) o : (due punti). Considerare gli esempi riportati di seguito:

   ```
   .*[$]
   ```

   ```
   .*[$>?:#]
   ```

   **Nota:** Quando si utilizza il simbolo del dollaro in un'espressione regolare, racchiuderlo tra parentesi quadre. Il simbolo del dollaro non compreso tra parentesi ha un significato speciale nelle espressioni regolari.

9. Fare clic su Salva e chiudi.
10. Fare clic su Salva.
11. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Informazioni su Esecuzione comando (a pagina 280)
Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Configurazione delle categorie operatore (a pagina 276)

## Configurazione di Esecuzione comando: Proprietà Telnet predefinite

La configurazione delle proprietà di Telnet predefinite comprende le attività seguenti:

- Configurazione della connettività
- Indicazione dello schema di accesso e dei dettagli correlati
- Indicazione per il cambio di utente una volta eseguito l'accesso all'host remoto
- Definizione dei dettagli per il cambio di utente

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Esecuzione comando e selezionare Modifica.
3. Nella scheda Proprietà Telnet predefinite, selezionare il pseudoterminale predefinito da richiedere sulla connessione di Telnet.
4. Selezionare la porta predefinita da utilizzare per connettersi all'host remoto.

   **Nota:** la porta 23 è la porta TCP/UDP di sistema per Telnet.

5. Per Timeout di connessione (sec), utilizzare la casella di selezione per selezionare l'intervallo, espresso in secondi, atteso dalla connessione prima del timeout.
6. Selezionare uno schema di accesso predefinito dall'elenco a discesa.
7. Definire i valori e i prompt di accesso predefiniti:
   a. Immettere un'espressione regolare per il prompt di accesso (ad esempio, immettere .*ogin.*:).
   b. Immettere il nome utente da utilizzare per accedere all'host remoto.
   c. Immettere un'espressione regolare per il prompt di testo predefinito per indicare che l'host remoto richiede una password per l'utente che esegue l'accesso (ad esempio, immettere .*assword.*:).
   d. Immettere la password predefinita da utilizzare durante l'accesso all'host remoto.
8. Immettere un'espressione regolare per il prompt dei comandi per indicare che l'host remoto è pronto per i comandi (ad esempio, immettere .*[$>?:#]).

   **Nota:** Per utilizzare il simbolo del dollaro in un'espressione regolare, racchiuderlo tra parentesi quadre. Ad esempio, [$].
9. Selezionare l'intervallo, espresso in secondi, atteso dalla connessione per l'invio dei comandi dal prompt.

10. Definire i valori predefiniti per il cambio di utente:

    a. Specificare se cambiare utente prima di eseguire lo script o i comandi specificati.

    b. Immettere il comando specifico del sistema operativo con cui cambiare utente sull'host remoto.

       **Nota:** Il comando "su -root" cambia l'utente con quello principale.

       Considerare gli esempi riportati di seguito:

       ```
       su - <username>
       ```

       ```
       sudo su - <username>
       ```

    c. Immettere un'espressione regolare per il prompt di testo predefinito relativo alla password per il cambio di utente (ad esempio, immettere .*assword.*:).

    d. Immettere la password predefinita per il prompt di testo della password.

    e. Immettere un'espressione regolare per il prompt per indicare che l'host remoto è pronto per i comandi, ad esempio il cambio di utente.

       **Nota:** I simboli cancelletto (#), maggiore (>) e punto interrogativo (?) sono prompt dei comandi standard. Immettere .*[$>?:#] per trovare una corrispondenza con qualsiasi valore immesso (incluse nuove righe) seguito dai simboli #, >, ?, $ o :.

       Considerare gli esempi riportati di seguito:

       ```
       .*[$]
       ```

       ```
       .*[$>?:#]
       ```

       **Nota:** Per utilizzare il simbolo del dollaro in un'espressione regolare, racchiuderlo tra parentesi quadre. Ad esempio, [$].

11. Fare clic su Salva e chiudi.

12. Fare clic su Salva.

13. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Informazioni su Esecuzione comando (a pagina 280)
Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Configurazione delle categorie operatore (a pagina 276)

# Configurazione di Esecuzione comando: Proprietà predefinite di esecuzione dei comandi UNIX

È possibile configurare proprietà di esecuzione predefinite per i comandi UNIX.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Esecuzione comando e selezionare Modifica.
3. Selezionare la scheda Proprietà predefinite di esecuzione dei comandi UNIX.
4. Immettere uno dei seguenti moduli di interpretazione del comando Shell da utilizzare come valore predefinito per il profilo e i comandi shell:

   `/bin/bash`

   `/bin/csh`

   `/bin/ksh`

5. Immettere il nome del file di script della shell predefinita da interpretare prima di avviare un processo utente per cui non è specificato alcun profilo.

   Il profilo può contenere qualsiasi comando non interattivo riconosciuto dall'interprete shell.

6. Specificare i valori predefiniti per le credenziali utente.

   a. Selezionare una delle opzioni seguenti per specificare che gli operatori di processo utilizzino l'opzione selezionata quando le credenziali utente non sono specificate:

      ■ (Impostazione predefinita) Il valore predefinito è l'utente con cui viene eseguito il touchpoint.

        Gli operatori di processo utilizzano le credenziali utente con cui viene eseguito il processo di agente o di orchestrator.

      ■ L'impostazione predefinita è quella dell'utente predefinito specificato.

        Gli operatori di processo utilizzano le credenziali utente configurate come utente predefinito e password predefinita.

      ■ Nessuna impostazione predefinita.

        Gli operatori di processo utilizzano le credenziali utente fornite in fase di runtime.

   b. Considerare le implicazioni quando si specificano valori predefiniti per l'ID utente e la password:

      ■ Per impedire agli utenti di definire e avviare processi attraverso CA Process Automation a cui altrimenti non hanno accesso, specificare un ID utente esclusivamente con le autorizzazioni necessarie.

      ■ Non inserire l'ID utente e la password per obbligare gli utenti a immettere tali valori quando avviano i processi tramite CA Process Automation.

   c. Se appropriato, inserire l'account shell predefinito da utilizzare all'avvio di processi utente privi di nome utente e password.

   d. Se appropriato, immettere la password per l'account utente di Shell.

      **Nota:** Le password che fanno parte delle configurazioni di Esecuzione comando sono protette e non possono essere modificate con un programma, utilizzate come riferimento o passate a metodi esterni.

   e. Immettere nuovamente la password predefinita per confermarla.

7. Considerare le implicazioni quando si specificano valori predefiniti per l'ID utente e la password:

   ■ Per impedire agli utenti di definire e avviare processi attraverso CA Process Automation a cui altrimenti non hanno accesso, specificare un ID utente esclusivamente con le autorizzazioni necessarie.

   ■ Non inserire l'ID utente e la password per obbligare gli utenti a immettere tali valori quando avviano i processi tramite CA Process Automation.

8. Se appropriato, inserire l'account shell predefinito da utilizzare all'avvio di processi utente privi di nome utente e password.

9. Se appropriato, immettere la password per l'account utente di Shell.

   **Nota:** Le password che fanno parte delle configurazioni di Esecuzione comando sono protette e non possono essere modificate con un programma, utilizzate come riferimento o passate a metodi esterni.

10. Immettere nuovamente la password predefinita per confermarla.
11. Indicare se caricare il profilo utente associato all'utente e alla password predefiniti specificati.
12. Indicare se disabilitare il controllo della password.
13. Fare clic su Salva e chiudi.
14. Fare clic su Salva.
15. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Informazioni su Esecuzione comando (a pagina 280)
Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Configurazione delle categorie operatore (a pagina 276)

## Configurazione di Esecuzione comando: Proprietà predefinite di esecuzione dei comandi Windows

È possibile configurare le proprietà di esecuzione predefinite per i comandi Windows.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Esecuzione comando e selezionare Modifica.
3. Selezionare la scheda Proprietà predefinite di esecuzione dei comandi Windows.
4. Immettere il modulo di interpretazione dei comandi shell da utilizzare per il profilo e per i comandi shell. Ad esempio:

   ```
   cmd.exe
   ```

   **Nota:** Non immettere Command.exe.

5. Immettere il nome del file di script della shell predefinita da interpretare prima di avviare un processo utente per cui non è specificato alcun profilo.

   L'interprete dei comandi specificato dal programma Shell interpreta il file del profilo. Il profilo può contenere qualsiasi comando non interattivo riconosciuto dall'interprete shell.

6. Specificare i valori predefiniti per le credenziali utente.

    a. Selezionare una delle opzioni seguenti per specificare che gli operatori di processo utilizzino l'opzione selezionata quando le credenziali utente non sono specificate:

        - (Impostazione predefinita) Il valore predefinito è l'utente con cui viene eseguito il touchpoint.

          Gli operatori di processo utilizzano le credenziali utente con cui viene eseguito il processo di agente o di orchestrator.

        - L'impostazione predefinita è quella dell'utente predefinito specificato.

          Gli operatori di processo utilizzano le credenziali utente configurate come utente predefinito e password predefinita.

        - Nessuna impostazione predefinita.

          Gli operatori di processo utilizzano le credenziali utente fornite in fase di runtime.

    b. Considerare le implicazioni quando si specificano valori predefiniti per l'ID utente e la password:

        - Per impedire agli utenti di definire e avviare processi attraverso CA Process Automation a cui altrimenti non hanno accesso, specificare un ID utente esclusivamente con le autorizzazioni necessarie.

        - Non inserire l'ID utente e la password per obbligare gli utenti a immettere tali valori quando avviano i processi tramite CA Process Automation.

    c. Se appropriato, inserire l'account shell predefinito da utilizzare all'avvio di processi utente privi di nome utente e password.

    d. Se appropriato, immettere la password per l'account utente di Shell.

       **Nota:** Le password che fanno parte delle configurazioni di Esecuzione comando sono protette e non possono essere modificate con un programma, utilizzate come riferimento o passate a metodi esterni.

    e. Immettere nuovamente la password predefinita per confermarla.

7. Considerare le implicazioni quando si specificano valori predefiniti per l'ID utente e la password:

    - Per impedire agli utenti di definire e avviare processi attraverso CA Process Automation a cui altrimenti non hanno accesso, specificare un ID utente esclusivamente con le autorizzazioni necessarie.

    - Non inserire l'ID utente e la password per obbligare gli utenti a immettere tali valori quando avviano i processi tramite CA Process Automation.

8. Se appropriato, inserire l'account shell predefinito da utilizzare all'avvio di processi utente privi di nome utente e password.

9. Se appropriato, immettere la password per l'account utente di Shell.

   **Nota:** Le password che fanno parte delle configurazioni di Esecuzione comando sono protette e non possono essere modificate con un programma, utilizzate come riferimento o passate a metodi esterni.

10. Immettere nuovamente la password predefinita per confermarla.
11. Indicare se caricare il profilo utente associato all'utente e alla password predefiniti specificati.
12. Fare clic su Salva e chiudi.
13. Fare clic su Salva.
14. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Informazioni su Esecuzione comando (a pagina 280)
Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Database

La categoria di operatori Database sfrutta la tecnologia JDBC (Java Database Connectivity). La tecnologia JDBC supporta la connettività in un ambiente eterogeneo tra il linguaggio di programmazione Java e i database come Microsoft SQL Server. La categoria Database non supporta operazioni amministrative quali l'interruzione di un server di database. È possibile fornire informazioni di connessione con il server, la porta e l'ID di sistema (SID), o una voce di TNSNAMES in tnsnames.ora. Il file tnsnames.ora è il file di configurazione di Oracle Service Name.

La categoria Database include impostazioni per i database seguenti:

- Oracle
- MSSQL
- MySQL
- Sybase

Per utilizzare la categoria di operatori Database con un RDBMS da un vendor diverso da quelli impiegati da CA Process Automation, installare il driver appropriato.

**Nota:** per informazioni, consultare la sezione Installazione dei driver JDBC per i connettori JDBC nella *Guida all'installazione.*

**Ulteriori informazioni:**

Abilitazione di Protezione integrata di Windows per il Modulo JDBC con server MSSQL (a pagina 294)

## Configurazione di database: Proprietà predefinite Oracle

È possibile configurare la categoria di operatori Database per Oracle.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Database e selezionare Modifica.
3. Nella scheda Proprietà predefinite Oracle, selezionare uno dei valori seguenti come il tipo predefinito di driver Oracle JDBC. Utilizzare una versione JDBC che corrisponde alla versione di Java Development Kit (JDK).

   **thin**

   Il tipo di driver Thin viene utilizzato sul lato client senza alcuna installazione di Oracle. Il thin driver si connette al database Oracle con socket Java.

   **oci**

   Il tipo di driver OCI viene utilizzato sul lato client con Oracle installato. I driver OCI utilizzano l'interfaccia Oracle Call Interface (OCI) per interagire con il database Oracle.

   **kprb**

   Il tipo di driver KPRB viene utilizzato per la scrittura di trigger e stored procedure di database Java.

4. Accettare la voce di driver predefinita (oracle.jdbc.OracleDriver) o modificarla.
5. Immettere la posizione del server di Oracle e le credenziali di accesso:
   a. Immettere il server host su cui è in esecuzione il database Oracle.
   b. Immettere la porta predefinita del database Oracle.
   c. Immettere il nome utente predefinito per l'utente di database Oracle.
   d. Immettere la password associata al nome utente specificato.
6. Immettere l'ID del servizio Oracle.
7. Immettere l'origine dei contenuti di tnsnames.ora nella directory di Oracle.

   Il file Oracle TNS Names converte un alias di database locale in informazioni che abilitano la connettività al database. Queste informazioni includono l'indirizzo IP, la porta e l'ID del servizio di database.

8. Accettare il numero massimo predefinito di righe da recuperare (10) o selezionare un altro valore fino a 512.

9. Immettere il metodo predefinito di crittografia dei dati. Considerare l'inserimento dei valori seguenti, dei quali RCA_128 e RCA_256 sono riferiti solo a edizioni nazionali:

   - RC4_40
   - RC4_56
   - RC4_128
   - RC4_256
   - DES40C
   - DES56C
   - 3DES112
   - 3DES168
   - SSL
   - AES128
   - AES256
   - AES192

10. Immettere il valore predefinito tratto dai checksum supportati da Oracle. Consultare la documentazione di Oracle.

11. Fare clic su Salva e chiudi.

12. Fare clic su Salva.

13. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Database (a pagina 290)
Configurazione delle categorie operatore (a pagina 276)

## Configurazione di database: Proprietà predefinite MS SQL Server

È possibile configurare la categoria di operatori Database per server MSSQL.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Database e selezionare Modifica.
3. Fare clic sulla scheda Proprietà predefinite MS SQL Server.
4. Accettare com.microsoft.sqlserver.jdbc.SQLServerDriver come driver predefinito per MS SQL Server.
5. Immettere il nome host o l'indirizzo IP dell'host su cui è in esecuzione MS SQL Server da utilizzare come valore predefinito.
6. Immettere la porta predefinita di MS SQL Server, in genere 1433.
7. Specificare le credenziali predefinite per l'utente di database MSSQL.
   - Immettere un nome utente.
   - Immettere la password associata al nome utente specificato.
8. Accettare il numero massimo predefinito di righe da recuperare (10) o selezionare un altro valore fino a 512.
9. Immettere il nome predefinito del database MSSQL.
10. Immettere il nome predefinito dell'istanza MS SQL.
11. Fare clic su Salva e chiudi.
12. Fare clic su Salva.
13. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Database (a pagina 290)
Configurazione delle categorie operatore (a pagina 276)

# Abilitazione di Protezione integrata di Windows per il Modulo JDBC con server MSSQL

È possibile abilitare gli operatori nella categoria Database per Microsoft SQL Server (MSSQL) per utilizzare la protezione integrata. Questi operatori possono utilizzare la protezione integrata durante la connessione ai touchpoint sugli host in esecuzione su sistemi operativi di Windows.

Un operatore Database appartiene alla categoria Database. Gli host di destinazione sono host con un agente o un orchestrator. Per ciascun host di destinazione accessibile a un operatore Database, copiare sqljdbc_auth.dll nel percorso di sistema dell'host. Questo processo consente di configurare la categoria Database per MSSQL in modo che utilizzi la protezione integrata con l'autenticazione di Windows.

È possibile abilitare Protezione integrata di Windows per la categoria Database per MSSQL Server.

**Attenersi alla procedura seguente:**

1. Se si utilizza la versione del driver di Microsoft SQL Server fornita con CA Process Automation, scaricare la versione 3.0 del driver dal sito Web di Microsoft. Altrimenti, individuare (o scaricare di nuovo) la versione completa del driver.
2. Individuare sqljdbc_auth.dll fornito o scaricato che corrisponde all'hardware su cui è in esecuzione l'agente o l'orchestrator.
3. Copiare sqljdbc_auth.dll in una cartella sul percorso di sistema di ciascun agente o orchestrator di CA Process Automation in esecuzione su un sistema operativo di Windows.

   Per determinare il percorso di sistema, eseguire *una* delle azioni seguenti:

   - Immettere il comando seguente nel prompt dei comandi:

     ```
     echo %PATH%
     ```

     Viene visualizzato il percorso di sistema.

   - Selezionare Start, Impostazioni, Pannello di controllo, Sistema, Avanzate (Impostazioni di sistema avanzate), Variabili d'ambiente. Il percorso di sistema è visualizzato nella variabile PATH.
4. Riavviare l'agente o l'orchestrator.

**Note:**

- Quando un utente crea un URL di connessione senza protezione integrata, specifica il nome utente e la password. Per utilizzare la protezione integrata, non specificare il nome utente e la password.
- Aggiungere ;integratedSecurity=true all'URL di connessione. Ad esempio:

  ```
  jdbc:sqlserver://localhost ... ;integratedSecurity=true
  ```

## Configurazione di database: Proprietà predefinite MySQL

È possibile configurare la categoria di operatori Database per server MySQL.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Database e selezionare Modifica.
3. Fare clic sulla scheda Proprietà predefinite server MSSQL.
4. Accettare com.mysql.jdbc.Driver come driver predefinito per MySQL.
5. Identificare l'host su cui è in esecuzione il database MySQL.
6. Immettere la porta predefinita del database MySQL, ad esempio 3306.
7. Immettere le credenziali di accesso predefinite per il database MySQL predefinito.
   a. Immettere il nome utente predefinito per l'utente di database MySQL.
   b. Immettere la password associata al nome utente specificato.
8. Accettare il numero massimo predefinito di righe da recuperare (10) o selezionare un altro valore fino a 512.
9. Immettere il nome predefinito del database MySQL.
10. Fare clic su Salva e chiudi.
11. Fare clic su Salva.
12. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Database (a pagina 290)
Configurazione delle categorie operatore (a pagina 276)

## Configurazione di database: Proprietà predefinite Sybase

È possibile configurare la categoria di operatori Database per Sybase.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Database e selezionare Modifica.

3. Fare clic sulla scheda Proprietà predefinite Sybase.
4. Selezionare uno dei valori seguenti per il sistema di database relazionale di Sybase predefinito:
   - Adaptive Server via Internet (ASA)
   - Adaptive Server Enterprise (ase)
5. Accettare Tds o immettere un protocollo di connessione predefinito diverso.
6. Accettare com.sybase.jdbc2.jdbc.SybDriver o immettere un driver predefinito diverso.
7. Specificare la posizione del database Sybase.
   a. Identificare l'host del server.
   b. Immettere la porta predefinita.
8. Immettere le credenziali di accesso predefinite per il database Sybase predefinito.
   a. Immettere il nome utente predefinito.
   b. Immettere la password associata al nome utente specificato.
9. Accettare 10 come numero massimo predefinito di righe da recuperare o selezionare un altro valore fino a 512.
10. Specificare la quantità di memoria utilizzata dal driver per memorizzare i dati senza distinzione dei risultati nei modi seguenti:

    **-1**

    Tutti i dati memorizzati nella cache.

    **0**

    Vengono memorizzati fino a 2 GB di dati nella cache.

    ***n***

    Definisce la dimensione di buffer in KB, in cui il valore è una potenza di 2 (un numero pari). Quando il limite specificato viene raggiunto, i dati vengono memorizzati nella cache.
11. Indicare se utilizzare il meccanismo compatibile con JDBC v3.0 come soluzione alternativa di prestazioni in batch predefinita.

    **Nota:** Se non è selezionato, viene utilizzato il meccanismo di batch nativo.
12. Fare clic su Salva e chiudi.
13. Fare clic su Salva.
14. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Database (a pagina 290)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Date-Time

Gli operatori nella categoria Data-Ora possono essere eseguiti su orchestrator. La categoria Data-Ora supporta opzioni di data e ora per operatori in altre categorie e operatori condizionali per l'esecuzione di rami di un processo. Seguono gli esempi:

- Confrontare la data e l'ora correnti con la data e l'ora specificate.
- Verificare se la data corrente è inclusa nella regola del calendario.
- Attendere la data e l'ora specificate.

La categoria di operatori Data-Ora non dispone di proprietà configurabili.

## Informazioni su Servizi directory

La categoria di operatori Servizi directory fornisce un'interfaccia per il supporto LDAP (Lightweight Directory Access Protocol). Gli operatori Servizi directory possono essere eseguiti su un orchestrator o un agente.

## Configurazione delle impostazioni predefinite dei Servizi directory

È possibile configurare Servizi directory. La categoria di operatore Servizi directory fornisce un'interfaccia per il supporto LDAP/AD.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Servizi directory e selezionare Modifica.
3. Specificare un valore predefinito di dimensioni batch per restituire i risultati dell'operazione per consentire al server di ottimizzare le prestazioni e l'utilizzo delle risorse. Selezionare un valore compreso tra 1 e 1000 oppure immettere 0 per consentire al server di determinare la dimensione batch.
4. Selezionare un valore per il numero massimo di oggetti da restituire durante l'esecuzione degli operatori Acquisisci oggetto o Acquisisci utente.

5. Specificare i nomi di classe factory seguenti:

    a. Accettare il valore predefinito, com.sun.jndi.ldap.LdapCtxFactory, come nome di classe completo per la classe factory che crea un contesto iniziale.

    b. Immettere un elenco separato da due punti di nomi completi per la classe factory di stato in grado di acquisire lo stato di un oggetto specificato. Non selezionare questo campo per utilizzare le classi factory di stato predefinite.

    c. Immettere un elenco separato da due punti di nomi di classe completi per le classi factory che creano un oggetto in base alle relative informazioni. Non selezionare questo campo per utilizzare le classi factory di oggetto predefinite.

6. Immettere un elenco separato da due punti di codici di lingua definiti in RFC 1766. Lasciare vuoto per consentire al server LDAP di determinare la lingua preferita.

7. Selezionare uno dei valori seguenti per specificare la modalità di gestione dei riferimenti con il server LDAP.

    **Ignore**

    Ignorare i riferimenti.

    **Follow**

    Seguire i riferimenti.

    **Throw**

    Restituire il primo riferimento che il server incontra e interrompere la ricerca.

8. Specificare il meccanismo di autenticazione per il server LDAP da utilizzare con una delle voci seguenti:

    **Nessuno**

    Non utilizzare alcuna autenticazione (anonimo).

    **Semplice**

    Utilizzare un metodo di autenticazione poco sicuro (password non crittografata). Selezionare questa opzione quando si imposta Protocollo di protezione su SSL.

    **Elenco di meccanismi SASL separato da spazi**

    Consentire a LDAP di supportare qualsiasi tipo di autenticazione accettato dal client e dal server LDAP.

9. Indicare il protocollo di protezione in uno dei modi seguenti:

    - Immettere **ssl** per indicare il protocollo che permette connessioni al server LDAP tramite un socket protetto.

      **Importante.** In caso di connessione ad Active Directory (AD), immettere **ssl** in *minuscolo*. Active Directory rifiuta il valore SSL.

    - Lasciare vuoto per utilizzare la connettività di base.

10. Selezionare un valore per indicare il timeout di connessione in secondi oppure immettere 0 (zero) per non inserire un timeout.
11. Immettere la posizione del server LDAP e le credenziali di accesso predefinite.
    a. Immettere il nome host o l'indirizzo IP.
    b. Immettere la porta predefinita del server LDAP. Considerare le porte seguenti:
        - 389: la porta ldap nota per il protocollo LDAP (Lightweight Directory Access Protocol).
        - 636: la porta ldaps per il protocollo LDAP su TLS/SSL.
    c. Immettere l'ID dell'utente LDAP predefinito. Gli operatori possono utilizzare il valore predefinito o sostituirlo.
    d. Immettere la password predefinita per l'utente LDAP. Gli operatori possono utilizzare il valore predefinito o sostituirlo.
12. Immettere il nome distinto di base predefinito (DN). Gli operatori possono utilizzare il valore predefinito o sostituirlo.
13. Immettere **uid** o **cn** come prefisso utente predefinito.
14. Fare clic su Salva e chiudi.
15. Fare clic su Salva.
16. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Servizi directory (a pagina 297)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Posta elettronica

La categoria di operatori Posta elettronica consente di lavorare con messaggi e cartelle su un server di posta. Gli operatori Posta elettronica comunicano con il server di posta in remoto utilizzando uno dei protocolli seguenti:

- Post Office Protocol versione 3 (POP3)
- POP3-SSL
- Protocollo IMAP (Internet Message Access Protocol)
- IMAP-SSL

Alcuni operatori, come quelli che agiscono su cartelle, vengono supportati solo con l'utilizzo del protocollo IMAP.

**Nota:** per informazioni sul protocollo supportato da ciascun operatore Posta elettronica, consultare la *Guida di riferimento per la progettazione dei contenuti*.

## Configurazione delle proprietà predefinite per i messaggi di posta elettronica

È possibile configurare delle impostazioni predefinite per gli operatori Posta elettronica.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Posta elettronica e selezionare Modifica.
3. Immettere il nome host del server SMTP per avvisi di posta elettronica Java.
4. Immettere l'indirizzo di posta elettronica da visualizzare nel campo del mittente per gli avvisi di posta elettronica in uscita di Java. Completare la configurazione dell'account. Ad esempio:

   `nomeutente@nome-azienda.com`

5. Selezionare il protocollo predefinito con cui ricevere messaggi di posta elettronica da un server remoto o da un server Web remoto.
   - IMAP
   - POP3
   - IMAP-SSL
   - POP3-SSL
6. Identificare il server di posta predefinito da cui viene recuperato il messaggio di posta elettronica.

7. Immettere la porta predefinita del server di posta predefinito per i messaggi di posta elettronica in entrata. Considerare le porte seguenti:

   **143**

   La porta IMAP per una connessione non protetta.

   **110**

   La porta POP3 per una connessione non protetta.

   **993**

   La porta IMAP-SSL per una connessione protetta.

   **995**

   La porta POP3-SSL per una connessione protetta.

8. Specificare le credenziali predefinite dell'utente di posta elettronica come segue o lasciare vuoto questo valore se è sempre specificato a livello di operatore.
   a. Immettere un nome utente.
   b. Immettere la password associata.
9. Fare clic su Salva e chiudi.
10. Fare clic su Salva.
11. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Posta elettronica (a pagina 300)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Gestione file

La categoria di operatori Gestione file può essere eseguita su un agente o un orchestrator. Gli operatori Gestione file monitorano la presenza o lo stato di un file o una directory. Inoltre, gli operatori Gestione file eseguono la ricerca di modelli specifici nei contenuti di un file. Le regole POSIX regolano i modelli sulla corrispondenza al modello di testo. Questa funzione può essere utilizzata per determinare l'ulteriore elaborazione di un processo. Ad esempio, gli operatori Gestione file possono attendere un file XML che contenga i modelli che richiedono l'elaborazione. Gestione file può cercare messaggi di errore nei contenuti dei file di log.

La categoria di operatori Gestione file esegue la ricerca per file o monitora i contenuti di un file sulla destinazione. I file possono trovarsi su un altro computer o un'altra unità di rete, ma devono essere visibili per gli operatori. Tutti gli operatori Gestione file (ad esempio, per la creazione di percorsi di directory o l'analisi dei contenuti di file) vengono eseguiti come amministratore o come l'utente che ha avviato il touchpoint.

Specifiche condizioni per il controllo o l'attesa includono:

- Aspetto di un file.
- L'assenza di un file.
- Condizioni della dimensione di un file.
- Ultima modifica data/ora.
- Esistenza di una stringa o di un modello in un file (sulla base di maschere POSIX).

**Ulteriori informazioni:**

Configurazione di Gestione file (a pagina 302)

## Configurazione di Gestione file

È possibile configurare le impostazioni predefinite per gli operatori nella categoria Gestione file. A meno che non sia indicato diversamente, i campi di riferimento sono validi sia per i sistemi operativi UNIX o Linux sia per quelli Microsoft Windows.

**Nota:** Per espandere un campo relativo a una voce della finestra Gestione file più lunga dello spazio fornito, fare clic con il tasto destro del mouse sul campo, quindi selezionare Espandi.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Gestione file e selezionare Modifica.

3. Completare i passaggi seguenti nella finestra Gestione file:

   a. Fare clic su Proprietà predefinite di gestione file Windows o Proprietà predefinite di gestione file UNIX in base al sistema operativo da configurare.

   b. Completare i campi seguenti se si imposta il campo Richiedi credenziali utente su Imposta in modo predefinito l'utente specificato a continuazione:

      - Utente
      - Password
      - Conferma password

   c. (UNIX) Definire la shell del sistema dell'operatore. Ad esempio, immettere uno dei valori seguenti per Shell:

      - /bin/bash
      - /bin/csh/
      - /bin/ksh

   d. (UNIX) Selezionare o deselezionare la casella di controllo Disabilita controllo password, a seconda se il prodotto deve verificare o meno la password utente quando cambia utente.

   e. Immettere il comando per la compressione di un file o di una directory nel campo Utilità di compressione. Ad esempio:

      ```
      WZZIP -P -r {0} {1}
      ```

      ```
      gzip -qrf {0}
      ```

      - {0} indica il nome del file compresso di output.
      - {1} indica il nome del file sorgente da comprimere.

   f. Immettere il comando per l'estrazione di un file o di una directory compressa nel campo Utilità di decompressione. Ad esempio:

      ```
      WZUNZIP -d -o -yO {0}
      ```

      ```
      gunzip -qrf {0}
      ```

      {0} indica il nome del file compresso da estrarre.

4. Fare clic su Salva e chiudi.

5. Fare clic su Salva.

6. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Informazioni su Gestione file (a pagina 302)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Trasferimento file

La categoria Trasferimento file agisce come un client del protocollo di trasferimento file (FTP, File Transfer Protocol) che supporta gli operatori del file remoto in un processo. È possibile eseguire gli operatori nella categoria Trasferimento file su orchestrator o su touchpoint agente. La categoria Trasferimento file supporta tutti i comandi supportati dall'FTP standard, tra cui:

- Trasferimenti di file a/da un host remoto che supporta il protocollo di trasferimento file (FTP; File Transfer Protocol).
- Recupero di informazioni di file/directory da un host remoto.
- Eliminazione di un file o di una directory.
- Ridenominazione di un file o di una directory.

Nessun prerequisito viene richiesto per gli operatori basati su FTP mediante FTP standard e server FTP standard. Per trasferimenti SFTP, utilizzare SSH2 e predisporre i touchpoint per comunicare con il computer del server SFTP in base a nome utente e password.

Stabilire una connessione SSH e impostare i certificati con un client SSH, prima di utilizzare SFTP. CA Technologies fornisce un client SSH di test per Windows, in modo che sia possibile stabilire la connessione iniziale. La maggior parte dei computer UNIX lo ha già. SFTP è vantaggioso in quanto si tratta di un protocollo protetto. Con SFTP, i dati vengono trasmessi attraverso un tunnel crittografato e le password sono autenticate.

## Configurazione di Trasferimento file

È possibile configurare delle impostazioni predefinite per tutti gli operatori nella categoria Trasferimento file. In tutti i casi, è possibile sostituire i valori configurati a livello di operatore. Per ulteriori informazioni, consultare la sezione Configurazione della categoria ed ereditarietà dell'operatore (a pagina 314).

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Trasferimento file e selezionare Modifica.
3. Nella finestra Trasferimento file, completare il campo Porta UDP predefinita per il servizio Trivial FTP (la porta 69 è il valore tipico).
4. Fare clic su Salva e chiudi.
5. Fare clic su Salva.
6. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)

## Informazioni su Gestione Java

Gli operatori Gestione Java possono essere eseguite su un agente o un orchestrator. Questi operatori eseguono attività varie su risorse Java ManagedBean (MBean) mediante la tecnologia Java Management Extensions (JMX). Gli operatori utilizzano un nome utente e una password specifici per connettersi a un URL del servizio JMX o a un server JMX su un host e una porta specificati.

Gli operatori specifici eseguono le attività seguenti:

- Recupero di attributi MBean.
- Richiamo di metodi MBean tramite i parametri specificati.
- Impostazione di valori di attributi MBean.

La categoria Gestione Java non dispone di proprietà configurabili.

## Informazioni su Utilità di rete

Gli operatori nella categoria Utilità di rete possono essere eseguiti su orchestrator e su agenti e possono interagire con periferiche SNMP o gestioni SNMP (ad esempio i gestori di rete). Gli operatori Utilità di rete determinano lo stato di un elemento di configurazione per una periferica IP.

Gli operatori Utilità di rete generano avvisi basati su SNMP (trap) per periferiche o gestori di rete. La categoria Utilità di rete è progettata per influire su un processo, non per implementare un monitoraggio di rete completo.

Gli utenti possono richiamare operatori da Utilità di rete per:

- Ottenere i valori delle variabili remote di MIB (Management Information Base) e utilizzarli nel processo (ad esempio, come parametri o come condizioni).
- Attendere le condizioni del valore delle variabili remote di MIB.
- Impostare le variabili remote di MIB per influenzare il comportamento dei dispositivi esterni.
- Inviare la trap di SNMP per la segnalazione di errori di report e di condizioni speciali a piattaforme di gestione SNMP (ad esempio, Tivoli, HP OpenView, o ISM).

Gli operatori Utilità di rete sono disponibili su host con sistemi operativi di Windows e UNIX. Utilità di rete identificano variabili MIB remote con i rispettivi ID oggetto (OID).

**Ulteriori informazioni:**

Configurazione di Utilità di rete (a pagina 306)

## Configurazione di Utilità di rete

È possibile configurare la categoria di operatori Utilità di rete.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Trasferimento file e selezionare Modifica.
3. Fare clic con il pulsante destro del mouse su Utilità di rete e selezionare Modifica.
4. Nel campo Frequenza di polling (sec), specificare la frequenza con cui un operatore Utilità di rete ottiene in modo sincrono l'ID oggetto periferica (OID SNMP) per una variabile SNMP.
5. Fare clic su Salva e chiudi.
6. Fare clic su Salva.

   Il processo di configurazione applica le modifiche a livello di modulo alla configurazione del prodotto.
7. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Utilità di rete (a pagina 305)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Controllo processo

È possibile eseguire gli operatori nella categoria Controllo processo solo su touchpoint dell'orchestrator. Gli operatori Controllo processo hanno le funzioni seguenti:

- Avviano e interpretano i processi di CA Process Automation
- Richiamano altre categorie per l'esecuzione degli operatori in un'istanza di oggetto di processo
- Applicano le dipendenze
- Monitorano le chiamate di categoria e indicano le modalità di esecuzione dei rami successivi di un processo sui risultati della chiamata

All'avvio di un processo, viene eseguita una copia (istanza) del processo. Le modifiche alla copia non influiscono sulle altre copie o sul processo originale. È possibile avviare un processo nei modi seguenti:

- Con l'Ambiente di progettazione moduli.
- Da una pianificazione.
- Da un altro processo.
- Da un'applicazione esterna con un trigger di CA Process Automation.
- Da un'applicazione esterna che utilizza chiamate SOAP. Consultare la *Guida di riferimento per le API dei servizi Web*.

In caso di architetture fortemente decentralizzate, si consiglia di definire gruppi logici delle categorie di operatori in un ambiente e di configurare Controllo processo su un touchpoint selezionato in ogni gruppo. In una tale configurazione, i processi vengono avviati sul touchpoint che esegue gli operatori Controllo processo per un gruppo. Configurare un touchpoint appositamente per l'esecuzione di processi per più gruppi. L'esecuzione dei processi in un'architettura decentralizzata offre i vantaggi seguenti:

- Riduce il carico sui singoli computer
- Riduce l'impatto di incidenti potenziali
- Riduce la quantità di dati scambiati sugli host remoti

**Ulteriori informazioni:**

Configurazione di Controllo processo (a pagina 308)

## Configurazione di Controllo processo

È possibile configurare l'impostazione predefinita per gli operatori nella categoria Controllo processo.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Controllo processo e selezionare Modifica.
3. Nella finestra Controllo processo, completare il campo Tempo di completamento delle interazioni utente (min).
4. Fare clic su Salva e chiudi.
5. Fare clic su Salva.
6. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Informazioni su Controllo processo (a pagina 307)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Utilità

La categoria Utilità nella scheda Moduli contiene i campi relativi all'operatore Richiama Java.

**Importante.** L'operatore Richiama Java viene eseguito solo su un agente e non può essere configurato per un orchestrator.

La categoria Utilità consente di specificare:

- I percorsi ai file jar esterni da caricare per impostazione predefinita per tutti gli operatori Richiama Java.
- Accesso predefinito.

Ciascun file jar specificato diventa disponibile per il codice Java eseguito dagli operatori Richiama Java. Le classi definite nei file jar a livello di operatore sostituiscono le stesse classi specificate nei file jar per la categoria Utilità.

Se configurati, i responsabili di progettazione possono utilizzare il logger nel contesto del codice. Ad esempio:

```
logger.debug()
logger.info()
```

È possibile decidere di configurare la registrazione, in cui i dati registrati non includono informazioni.

## Configurazione di Utilità

È possibile configurare le impostazioni predefinite dell'operatore Richiama Java nella categoria Utilità solo se l'operatore viene eseguito su un agente. In caso contrario, questa categoria di operatore non richiede alcuna configurazione. L'operatore Richiama Java non può essere eseguito sugli orchestrator.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Utilità e selezionare Modifica.

   Viene visualizzata la scheda delle proprietà predefinite dell'operatore Richiama Java
3. Selezionare la casella di controllo Usare la modalità Java strict per applicare dichiarazioni variabili tipizzate, argomenti di metodo e tipi restituiti nel codice del metodo principale in fase di runtime.
4. Fare clic su Aggiungi parametro e definire i file JAR esterni se necessario.

5. Per rimuovere un file JAR selezionato, selezionare un elemento dall'elenco File JAR esterni, quindi fare clic su Elimina.
6. Compilare i campi rimanenti nella finestra Utilità se necessario.
7. Fare clic su Salva e chiudi.
8. Fare clic su Salva.
9. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Configurazione delle categorie ed ereditarietà degli operatori (a pagina 314)
Configurazione delle categorie operatore (a pagina 276)

## Informazioni su Servizi Web

Gli operatori Servizi Web vengono eseguiti su orchestrator e agenti. Due operatori forniscono un'interfaccia ai servizi remoti visualizzati mediante SOAP. Ognuno di questi operatori:

- Genera una richiesta di SOAP.

  I dati possono essere estratti in runtime dalle variabili e dai set di dati di CA Process Automation esistenti oppure da origini esterne.

- Invia la richiesta di SOAP alla categoria di operatori Servizi Web specificata in fase di progettazione o di runtime.
- Recupera le condizioni di errore di gestione della risposta, come appropriato.
- Analizza la risposta in arrivo e archivia i risultati nei set di dati di CA Process Automation a cui accedono gli operatori successivi in un processo.
- Una chiamata asincrona invia la richiesta e, dopo la ricezione di un riconoscimento, attende una risposta da una destinazione remota. Le chiamate asincrone utilizzano un meccanismo di invio e ricezione più complesso rispetto alle chiamate sincrone. Gli operatori successivi in un processo accedono ai dati restituiti.

Inoltre, la categoria Servizi Web offre la possibilità di automatizzare le funzionalità di gestione dei dati su una rete mediante HTTP. Ad esempio, i responsabili di progettazione dei contenuti possono sviluppare processi per l'automazione dei servizi RESTful tramite operatori HTTP. Quando un operatore HTTP viene configurato con un campo vuoto, tale operatore eredita il valore predefinito del campo corrispondente dall'impostazione della categoria principale. Pertanto, quando si fa una selezione per un campo della categoria di operatori, niente viene abilitato o disabilitato. È possibile specificare tutti i valori predefiniti, a propria discrezione. Quando si configurano queste stesse opzioni a livello di operatore, la selezione di un'opzione disabilita le altre.

**Ulteriori informazioni:**

Configurazione di Servizi Web (a pagina 311)

## Configurazione di Servizi Web

È possibile configurare le impostazioni predefinite per operatori nella categoria Servizi Web.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su Servizi Web e selezionare Modifica.
3. Nella finestra Servizi Web, fare clic su Proprietà predefinite dei servizi Web, quindi rivedere o aggiornare i campi se necessario.
4. Fare clic su Proprietà HTTP predefinite dei servizi Web, quindi rivedere o aggiornare i campi se necessario.
5. Fare clic su Salva e chiudi.
6. Fare clic su Salva.
7. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Categorie operatore e dove gli operatori vengono eseguiti (a pagina 321)
Sostituzione delle impostazioni ereditate da una categoria di operatori (a pagina 318)
Informazioni su Servizi Web (a pagina 310)
Configurazione delle categorie operatore (a pagina 276)

# Configurazione dei valori per un gruppo di operatori personalizzati

È possibile configurare i valori delle variabili definite per un gruppo di operatori personalizzati selezionato. I gruppi di operatori personalizzati vengono definiti nella scheda Configurazione del gruppo dell'editor di un operatore personalizzato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Moduli, fare clic con il pulsante destro del mouse su un gruppo di operatori personalizzati e selezionare Modifica.

   Viene visualizzato il gruppo di operatori personalizzati selezionato. Il prodotto visualizza inizialmente le pagine e le variabili senza valori.
3. Per ciascun campo visualizzato o matrice, aggiungere il valore da utilizzare come predefinito.

   È possibile sostituire i valori predefiniti a livello di ambiente e di operatore.
4. Fare clic su Salva e chiudi.
5. Fare clic su Salva.
6. Terminata la configurazione delle categorie di operatori e dei gruppi di operatori personalizzati nella scheda Moduli, selezionare Dominio e fare clic su Sblocca.

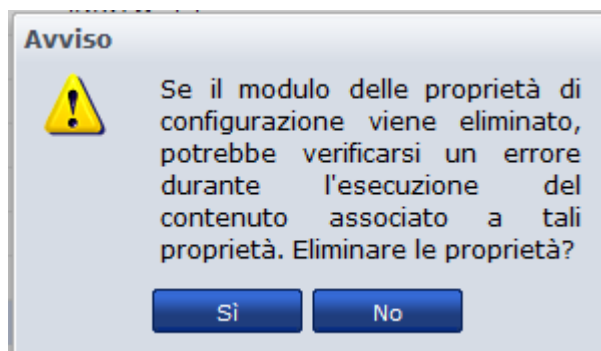
**Nota:** Quando si elimina una variabile o si modifica il tipo di dati della variabile, il prodotto non pubblica i cambiamenti nel dominio o negli ambienti associati.

# Eliminazione della configurazione di un gruppo di operatori personalizzati

Gli amministratori possono utilizzare la scheda Moduli del browser di configurazione per eliminare il gruppo pubblicato di operatori personalizzati dal dominio e dai relativi ambienti.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il tasto destro del mouse sul dominio e selezionare Blocca.
3. Fare clic con il pulsante destro del mouse sul gruppo di operatori personalizzati e selezionare Elimina.

   Viene visualizzato il seguente avviso:

   
   

4. Fare clic su Sì per confermare l'eliminazione.

   CA Process Automation elimina il modulo di configurazione del gruppo di operatori personalizzati dal dominio. Se un processo utilizza quel modulo di configurazione del gruppo di operatori personalizzati, l'esecuzione non riesce.

5. Fare clic su Salva.

   La configurazione del gruppo di operatori personalizzati viene eliminata dal dominio e dai relativi ambienti.

# Configurazione delle categorie ed ereditarietà degli operatori

Le categorie dell'operatore, come Posta elettronica o Trasferimento file, presentano impostazioni configurabili con valori predefiniti. Gli amministratori possono modificare una categoria dalla scheda Moduli a diversi livelli della gerarchia di dominio. In fase di installazione, le impostazioni predefinite per ciascuna categoria operatore iniziano a livello di dominio. Queste impostazioni vengono contrassegnate come Eredita dal dominio a livello di ambiente. A livello di orchestrator, queste impostazioni vengono contrassegnate come Eredita dall'ambiente.

Come illustrato di seguito, le impostazioni della categoria dell'operatore vengono ereditate dal dominio per ogni ambiente e da ogni ambiente per gli orchestrator in tale ambiente. Le impostazioni del modulo sono sostituibili a livello di dominio, a livello di ambiente e a livello di orchestrator.

Gli operatori che utilizzano come destinazione un orchestrator ereditano le impostazioni per la categoria operatore da tale orchestrator. Se necessario i responsabili di progettazione dei contenuti sovrascrivono queste impostazioni ereditate a livello di operatore.

Gli agenti ereditano le impostazioni configurate a livello di dominio, ma gli operatori non utilizzano queste impostazioni. Quando un touchpoint è associato a un agente, l'associazione include un ambiente. Durante il runtime, gli operatori che impostano come destinazione un touchpoint utilizzano le proprietà configurate per l'ambiente associato a tale touchpoint.

**Nota:** per i gruppi di operatori personalizzati definiti dall'utente, le impostazioni vengono ereditate dal livello di dominio a quello di ambiente. Gli amministratori possono sostituire a livello di ambiente le impostazioni definite a livello di dominio. Non è possibile sostituire queste impostazioni a livello di orchestrator o di agente.

**Ulteriori informazioni:**

Categorie dell'operatore e cartelle dell'operatore (a pagina 272)

# Abilitazione o disabilitazione di una categoria operatore

In genere le impostazioni della categoria operatore sono configurate a livello di dominio. Per impostazione predefinita, le impostazioni della categoria operatore per gli ambienti sono configurate su Eredita dal dominio. Per impostazione predefinita, le impostazioni della categoria operatore per gli orchestrator e gli agenti sono impostate su Eredita dall'ambiente.

Accedere alla scheda Moduli di un ambiente, un orchestrator o un agente per:

- Abilitare una o più categorie operatore.
- Disabilitare una o più categorie operatore.
- Configurare una o più categorie abilitate.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.

   Si apre il Browser di configurazione.

2. Eseguire una delle azioni seguenti per inserire un blocco al livello desiderato:
   - Espandere il nodo Dominio, selezionare l'ambiente di destinazione e fare clic su Blocca.
   - Espandere il nodo Orchestrator, selezionare l'orchestrator di destinazione e fare clic su Blocca.
   - Espandere il nodo Agenti, selezionare l'agente di destinazione e fare clic su Blocca.
3. Fare clic sulla scheda Moduli.
4. Selezionare una categoria operatore, fare clic sulla colonna Attiva/Disattiva e selezionare o Abilitato o Disabilitato.
5. Fare clic su Salva.
6. Fare clic su Sblocca.

# Abilitazione o disabilitazione di un gruppo di operatori personalizzati

In genere le impostazioni del gruppo di operatori personalizzati sono configurate a livello di dominio. Per impostazione predefinita, le impostazioni del gruppo di operatori personalizzati per gli ambienti sono configurate su Eredita dal dominio.

Accedere alla scheda Moduli di un ambiente per:

- Abilitare uno o più gruppi di operatori personalizzati.
- Disabilitare uno o più gruppi di operatori personalizzati.
- Sostituire le impostazioni di uno o più gruppi abilitati.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.

   Si apre il Browser di configurazione.

2. Espandere il nodo Dominio, selezionare l'ambiente di destinazione e fare clic su Blocca.
3. Fare clic sulla scheda Moduli.
4. Selezionare un gruppo di operatori personalizzati, fare clic sulla colonna Abilita/Disabilita e selezionare Abilitato o Disabilitato.
5. Fare clic su Salva.
6. Fare clic su Sblocca.

# Sostituzione delle impostazioni ereditate da una categoria di operatori

Un amministratore con diritti di Amministratore di dominio configura le categorie per gli operatori a livello di dominio. Un amministratore con diritti Amministratore della configurazione di ambiente può sostituire le impostazioni ereditate ai seguenti livelli:

- Ambiente
- orchestrator
- agente

Le impostazioni della categoria operatore configurate a livello di dominio vengono visualizzate come Eredita dal dominio. Questa impostazione si trova all'interno di un elenco a discesa, in cui è possibile selezionare anche Abilitato e Disabilitato. Selezionare Abilitato per modificare le impostazioni ereditate. Selezionare Disabilitato per disabilitare gli operatori nella categoria selezionata.

È possibile sostituire le impostazioni ereditate per qualsiasi categoria di operatori a uno o più livelli.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. (Facoltativo) Sostituire le impostazioni selezionate a livello di ambiente come segue:
    a. Fare clic con il pulsante destro del mouse sull'ambiente selezionato, quindi selezionare Blocca.
    b. Fare clic sulla scheda Moduli.
    c. Selezionare una categoria, fare clic sull'elenco a discesa per Attiva/Disattiva e selezionare Abilitato.
    d. Fare clic con il tasto destro del mouse sulla categoria e selezionare Modifica.

       Le proprietà della categoria selezionata vengono visualizzate in un elenco scorrevole.
    e. Modificare una o più impostazioni ereditate.
    f. Fare clic su Salva.
    g. Fare clic con il pulsante destro del mouse sull'ambiente e selezionare Sblocca.

3. (Facoltativo) Eseguire la sostituzione delle impostazioni selezionate a livello di orchestrator come segue:
   a. Espandere Orchestrator, selezionare un orchestrator e fare clic su Blocca.
   b. Fare clic sulla scheda Moduli.
   c. Selezionare una categoria, fare clic sull'elenco a discesa per Attiva/Disattiva e selezionare Abilitato.
   d. Fare clic con il tasto destro del mouse sulla categoria e selezionare Modifica.

      Le proprietà della categoria selezionata vengono visualizzate in un elenco scorrevole.
   e. Modificare una o più impostazioni ereditate.
   f. Fare clic su Salva.
   g. Fare clic su Sblocca.
4. (Facoltativo) Sostituire le impostazioni selezionate a livello di agente come segue:
   a. Espandere il nodo Agenti, selezionare un agente e fare clic su Blocca.
   b. Fare clic sulla scheda Moduli.
   c. Selezionare una categoria, fare clic sull'elenco a discesa per Attiva/Disattiva e selezionare Abilitato.
   d. Fare clic con il tasto destro del mouse sulla categoria e selezionare Modifica.

      Le proprietà della categoria selezionata vengono visualizzate in un elenco scorrevole.
   e. Modificare una o più impostazioni ereditate.
   f. Fare clic su Salva.
   g. Fare clic su Sblocca.

**Ulteriori informazioni:**

Configurazione di Utilità di rete (a pagina 306)
Configurazione di Servizi Web (a pagina 311)
Configurazione di Controllo processo (a pagina 308)
Configurazione di Gestione file (a pagina 302)
Configurazione di Esecuzione comando: Proprietà Telnet predefinite (a pagina 283)

# Sostituzione dei valori ereditati per un gruppo di operatori personalizzati

Un amministratore con diritti di amministratore di dominio configura i gruppi di operatori personalizzati a livello di dominio. Un amministratore con diritti di amministratore della configurazione di ambiente può sostituire le impostazioni ereditate a livello di ambiente.

**Nota:** a differenza delle categorie di operatore, non è possibile sostituire i valori dei gruppi di operatori personalizzati a livello di orchestrator o di agente.

Le impostazioni del gruppo di operatori personalizzati configurate a livello di dominio vengono visualizzate come Eredita dal dominio. Questa impostazione si trova all'interno di un elenco a discesa, in cui è possibile selezionare anche Abilitato e Disabilitato. Selezionare Abilitato per modificare le impostazioni ereditate. Selezionare Disabilitato per disabilitare gli operatori personalizzati nel gruppo selezionato.

È possibile sostituire le impostazioni ereditate nell'ambiente selezionato dal dominio.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic con il pulsante destro del mouse sull'ambiente selezionato, quindi selezionare Blocca.
3. Fare clic sulla scheda Moduli.
4. Selezionare una categoria, fare clic sull'elenco a discesa per Abilita/Disabilita e selezionare Abilitato.
5. Fare clic con il pulsante destro del mouse sulla categoria e selezionare Modifica.

   Le proprietà della categoria selezionata vengono visualizzate in un elenco scorrevole.
6. Modificare una o più impostazioni ereditate.
7. Fare clic su Salva.
8. Fare clic con il pulsante destro del mouse sull'ambiente e selezionare Sblocca.

**Ulteriori informazioni:**

Configurazione di Utilità di rete (a pagina 306)
Configurazione di Servizi Web (a pagina 311)
Configurazione di Controllo processo (a pagina 308)
Configurazione di Gestione file (a pagina 302)
Configurazione di Esecuzione comando: Proprietà Telnet predefinite (a pagina 283)

# Categorie operatore e dove gli operatori vengono eseguiti

Alcuni operatori vengono eseguiti solo sugli orchestrator, ma non sui touchpoint associati agli agenti. Altri operatori vengono eseguiti sugli orchestrator e sui touchpoint dell'agente, ma non sugli host remoti utilizzati come destinazione dai touchpoint proxy o gruppi host. Molti operatori possono essere eseguiti su qualsiasi tipo di destinazione. Alcuni operatori che rientrano in una categoria operatore possono essere eseguiti su orchestrator ma non sui touchpoint dell'agente. Altri operatori che rientrano nella stessa categoria possono essere eseguiti sia sugli orchestrator sia sui touchpoint dell'agente. Nella categoria operatore non viene eseguito un mapping perfetto della capacità di esecuzione su un determinato tipo di destinazione.

**Nota:** per informazioni sulle destinazioni valide per ciascun operatore, consultare la sezione relativa alle posizioni di esecuzione degli operatori della *Guida di riferimento per la progettazione del contenuto*.

**Ulteriori informazioni:**

Utilizzare un touchpoint proxy (a pagina 251)
Abilitazione o disabilitazione di una categoria operatore (a pagina 316)

# Capitolo 13: Amministrazione di trigger

Le applicazioni che non possono effettuare chiamate di SOAP possono utilizzare i trigger come alternativa. È consigliato l'utilizzo di chiamate di SOAP rispetto ai trigger, perché più efficiente.

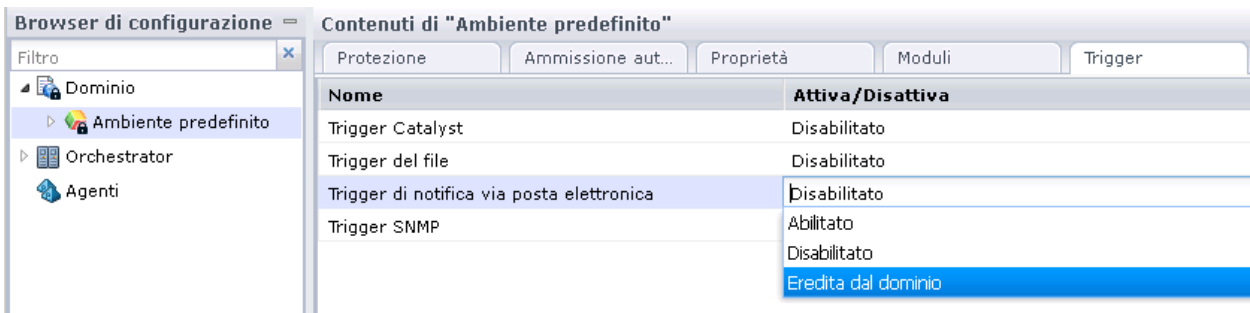
I trigger consentono applicazioni esterne per avviare un processo in CA Process Automation. Un trigger richiama il processo di CA Process Automation definito nel contenuto XML o in una trap di SNMP. Il contenuto XML può essere inviato alla posizione del file di configurazione o all'indirizzo di posta elettronica configurato. Il contenuto della trap di SNMP viene inviato a un OID che corrisponde a una espressione regolare configurata. CA Process Automation rileva trap di SNMP in arrivo nella porta della trap di SNMP configurata, la 162, per impostazione predefinita.

Questa sezione contiene i seguenti argomenti:

# Modalità di configurazione e utilizzo di trigger

Per applicazioni esterne che non sono in grado di rilasciare chiamate SOAP per avviare i processi di CA Process Automation, CA Process Automation fornisce quattro trigger predefiniti. È possibile configurare i trigger per abilitare l'inizializzazione di processi da uno dei seguenti:

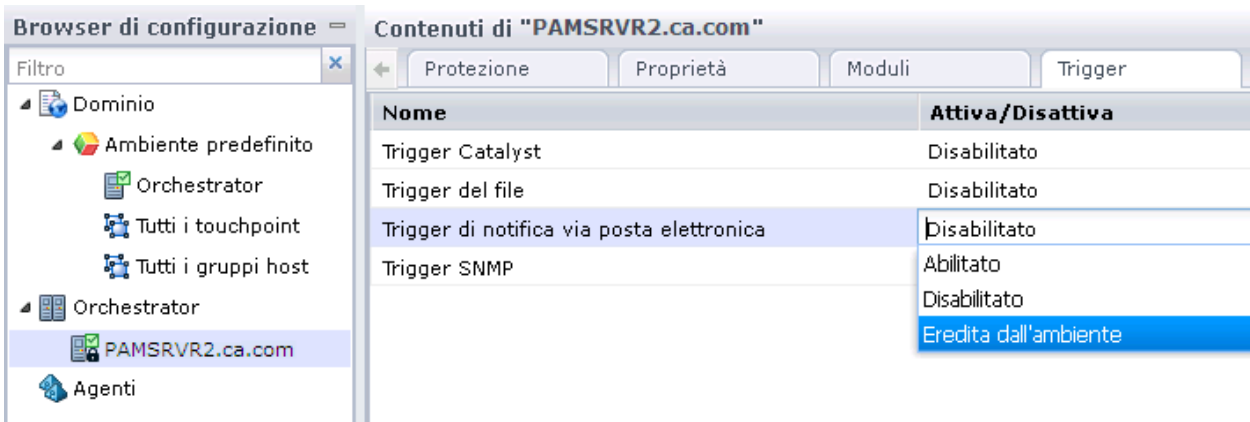
- Un evento da un connettore Catalyst
- Un file ricevuto
- Un messaggio di posta elettronica
- Un trap SNMP

Dopo aver configurato un trigger del file o di notifica via posta elettronica, è possibile creare contenuti XML. I contenuti XML avviano processi configurati di CA Process Automation con parametri dalle applicazioni esterne. Il contenuto XML può essere inserito in un file e posizionato nella directory configurata o inviato come messaggio di posta elettronica all'account configurato. Il trigger richiama il processo specificato nel contenuto XML quando vengono soddisfatti i criteri specificati. L'istanza di processo richiamata dal trigger popola anche i set di dati del processo con i valori specificati nel contenuto XML.

Dopo aver configurato un trigger della trap di SNMP in CA Process Automation, le applicazioni esterne possono inviare trap di SNMP a CA Process Automation. Quando CA Process Automation riceve un trap SNMP che corrisponde agli ID oggetto (OID) e al filtro dei valori di payload, il processo configurato si avvia. Il set di dati del processo attivato riceve le informazioni sul trap.

Dopo aver configurato la sottoscrizione ad un evento Catalyst, i connettori Catalyst esterni possono inviare eventi a CA Process Automation. Quando CA Process Automation riceve un evento Catalyst che corrisponde al filtro, il processo configurato si avvia con le proprietà di evento disponibili nel set di dati di processo.

A differenza delle impostazioni che l'ambiente eredita dal dominio per impostazione predefinita, i trigger sono disabilitati, per impostazione predefinita, sia a livello di ambiente sia a livello di orchestrator. Per abilitare trigger di CA Process Automation impostati a livello di dominio, impostare l'ereditarietà dal dominio a livello di ambiente. Quindi, impostare l'ereditarietà dall'ambiente a livello di orchestrator. In alternativa, è possibile sostituire i valori ereditati e configurare i valori dei trigger a livello di ambiente e di orchestrator.

Utilizzare il seguente approccio per implementare trigger:

1. Configurazione dei trigger a livello di dominio. Tali configurazioni non vengono ereditate per impostazione predefinita. Configurare i trigger solo se si desidera accettare l'avvio del processo da applicazioni esterne e solo per i tipi di trigger che si desidera ricevere.
2. A livello di ambiente, dove lo stato del trigger è Disabilitato, effettuare una delle seguenti operazioni:
   - Lasciarlo disabilitato per i tipi di trigger non applicabili.
   - Modificare lo stato in Eredita dal dominio per ambienti in cui la configurazione del dominio è applicabile.

   - Modificare lo stato in Abilitato e configurare i trigger a questo livello, se necessario.
3. A livello di orchestrator, dove lo stato del trigger è Disabilitato, effettuare una delle seguenti operazioni:
   - Lasciarlo disabilitato per i tipi di trigger non applicabili.
   - Modificare lo stato in Eredita da ambiente. Se si seleziona questa opzione, i valori sono desunti dall'ambiente in fase di runtime, se i trigger sono definiti a livello di ambiente. Altrimenti, vengono utilizzati i valori definiti a livello di dominio.

   - Modificare lo stato in Abilitato e modificare le proprietà.

4. CA Process Automation cerca la directory configurata, l'account di posta elettronica configurato, e la porta configurata per il contenuto che corrisponde ai relativi criteri di trigger.

   ■ Applicazioni esterne creano l'input per trigger configurati:

     – Per un trigger di file o trigger di posta, creare contenuto XML valido. Il contenuto XML specifica il percorso al processo in avvio, le credenziali, il tempo per l'avvio e i valori di parametro di inizializzazione.

     – Per un trigger di trap di SNMP, questi inviano una trap di SNMP valida alla porta 162 con valori che soddisfano il criterio configurato.

   ■ Le applicazioni esterne inviano i trigger a CA Process Automation come parte dell'elaborazione dell'automazione.

5. CA Process Automation elabora il nuovo contenuto e avvia il processo di CA Process Automation configurato con i valori passati dall'applicazione esterna.

6. Monitoraggio dell'istanza di processo richiamata tramite il trigger inviato dal processo esterno. È possibile monitorare il processo in esecuzione tramite la visualizzazione del processo. È possibile visualizzare i valori passati tramite il trigger nella pagina contenente le variabili del set di dati per il tipo di trigger associato.

**Ulteriori informazioni:**

Configurazione delle proprietà di trigger di file a livello di dominio (a pagina 329)
Configurazione delle proprietà di trigger di SNMP a livello di dominio (a pagina 334)
Attivazione di trigger per un orchestrator (a pagina 188)
Configurazione delle proprietà di trigger di posta a livello di dominio (a pagina 330)
Configurazione delle proprietà di trigger Catalyst a livello di dominio. (a pagina 326)

# Configurazione delle proprietà di trigger Catalyst a livello di dominio.

I diritti di amministratore di dominio consentono di configurare le proprietà del trigger Catalyst a livello di dominio. Con le proprietà del trigger Catalyst ereditate, il prodotto può avviare i processi quando riceve un evento Catalyst.

Il trigger Catalyst supporta un elenco di sottoscrizioni che fanno riferimento a connettore Catalyst con un filtro. Quando il prodotto riceve un evento corrispondente dal connettore Catalyst, avvia il processo specificato.

È possibile configurare le proprietà del trigger Catalyst a livello di dominio.

**Nota:** Questa procedura mostra alcuni esempi dell'impostazione di un trigger Catalyst affinché avvii un processo quando Microsoft System Center Operations Manager crea o aggiorna un oggetto Avviso. Le proprietà dell'oggetto Avviso sono disponibili come variabili di processo.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Trigger.
3. Fare clic con il tasto destro del mouse su Trigger Catalyst, quindi fare clic su Modifica.
4. Nella finestra di dialogo Trigger Catalyst, fare clic su Aggiungi parametro .
5. Nella finestra Sottoscrizioni Catalyst, fare clic sulla scheda MDR, quindi completare i campi se necessario.
6. Verificare che le voci immesse siano analoghe all'esempio seguente:

7. Fare clic sulla scheda Sottoscrizione, quindi completare i campi se necessario.
8. Verificare che le voci immesse siano analoghe all'esempio seguente:

9. Fare clic sulla scheda Filtri, quindi completare i campi se necessario.

10. Verificare che le voci immesse siano analoghe all'esempio seguente:

11. Fare clic sulla scheda Protezione Catalyst.
12. Immettere le credenziali nei campi Nome utente e Password.
13. Per ogni attestazione da aggiungere, fare clic sul pulsante Aggiungi parametro in Attestazioni, quindi completare i campi Nome attestazione e Valore attestazione.
14. Per ogni attestazione password da aggiungere, fare clic sul pulsante Aggiungi parametro in Attestazioni password, quindi completare i campi Nome attestazione e Valore attestazione.
15. Fare clic su Salva e chiudi.

    Il prodotto aggiunge la sottoscrizione che è stata definita all'elenco Sottoscrizione. Per modificare la definizione, evidenziare la voce e fare clic su Modifica.
16. Fare clic su Salva.
17. Selezionare Dominio e fare clic su Sblocca.

# Configurazione delle proprietà di trigger di file a livello di dominio

I diritti di amministratore di dominio consentono di configurare le proprietà del trigger del file a livello di dominio. L'ereditarietà *non* è il valore predefinito. Pertanto, per utilizzare le impostazioni configurate a livello di dominio, configurare Eredita dal dominio a livello di ambiente ed Eredita dall'ambiente a livello di orchestrator.

Quando si utilizzano i trigger del file per avviare i processi, l'orchestrator cerca i nuovi file nella directory di input specificata in conformità agli intervalli configurati. Il prodotto analizza il contenuto di ciascun file che corrisponde al modello del nome del file di input specificato e attiva il processo specificato. Dopo aver attivato il processo, il prodotto sposta il file nella directory elaborata specificata. Se il prodotto non riesce ad avviare il processo, sposta il file di attivazione e un file .err nella directory di errore specificata. Il file .err descrive le cause del mancato avvio.

**Nota:** Se un nuovo file presenta lo stesso nome di un file esistente, sostituire il file meno recente.

Prima di configurare le proprietà del trigger del file, creare le directory seguenti:

- Una directory di input con le autorizzazioni di scrittura necessarie per accettare file del trigger. Per permettere l'attivazione remota, considerare l'associazione della directory a una cartella FTP.
- Una directory elaborata per ricevere l'output elaborato correttamente.
- Una directory di errore per l'output che non può essere elaborato correttamente.

Se le directory non esistono, il prodotto le crea.

È possibile configurare le proprietà del trigger del file a livello di dominio.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Trigger, fare clic con il pulsante destro del mouse su Trigger del file e fare clic su Modifica.
3. Nella finestra di dialogo Trigger del file, completare i campi se necessario.

4. Verificare che i dati immessi siano validi. L'esempio seguente contiene voci valide.

5. Fare clic su Salva e chiudi.
6. Fare clic su Salva.
7. Selezionare Dominio e fare clic su Sblocca.

# Configurazione delle proprietà di trigger di posta a livello di dominio

I diritti di amministratore di dominio consentono di configurare le proprietà del trigger di notifica via posta elettronica a livello di dominio. Le proprietà dei trigger di notifica via posta elettronica abilitano l'attivazione dei processi solo se ereditate o configurate a livelli inferiori. Per eseguire l'eredità, configurare Eredita dal dominio a livello di ambiente ed Eredita dall'ambiente a livello di orchestrator.

Se attivo, il trigger di notifica via posta elettronica cerca nell'account di posta elettronica (configurato come nome utente e password) i messaggi di posta elettronica. Se il testo del messaggio di posta elettronica o un allegato contiene contenuto XML valido, il prodotto lo elabora. I parametri creati dal prodotto nell'istanza di processo attivata variano a seconda se il messaggio di posta elettronica contiene o meno del contenuto XML valido.

Prima di configurare le proprietà del trigger di notifica via posta elettronica, completare le attività seguenti:

- Creare un account di posta elettronica dedicato alla ricezione di messaggi di posta elettronica che attivano i processi.
- Verificare che il servizio IMAP sia abilitato sul server di posta come server di posta in arrivo.

  Se l'abilitazione del servizio IMAP è limitata dal server di posta aziendale, creare un server di posta proxy con IMAP abilitato. Specificare il server proxy come il server di posta in arrivo. Quindi, configurare il server di posta elettronica aziendale per inoltrare i messaggi di posta elettronica che sono indirizzati all'account utente configurato per il server di posta proxy.
- (Facoltativo) Creare un processo dell'orchestrator di dominio predefinito e salvarlo nel percorso del gestore di processo predefinito. Il prodotto utilizza il processo predefinito solo se il messaggio di posta elettronica non contiene contenuto XML valido. In questo caso, il processo viene avviato e inserisce le seguenti variabili nella pagina di SMTP nel set di dati di processo:

  **senderAdd**

  Identifica l'indirizzo di posta elettronica del mittente.

  **senderTime**

  Identifica l'ora del server di posta elettronica in cui il messaggio di posta elettronica è stato inviato.

  **MailBody**

  Contiene il contenuto completo del messaggio di posta elettronica.

  Il processo predefinito determina ogni ulteriore azione.

È possibile configurare le proprietà del trigger di notifica via posta elettronica a livello di dominio.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Trigger, fare clic con il pulsante destro del mouse su Trigger di notifica via posta elettronica, quindi fare clic su Modifica.

3. Nella finestra di dialogo Trigger di notifica via posta elettronica, scheda Proprietà generali, completare i campi se necessario.

   **Processo di attivazione predefinito (solo orchestrator)**

   Specifica la procedura per gestire i messaggi di posta elettronica con contenuto XML non valido nel testo del messaggio o nell'allegato.

   **Valori:**

   - **Campo vuoto**: i messaggi di posta elettronica senza contenuto di attivazione XML valido vengono ignorati.
   - Il percorso completo del processo da avviare con l'orchestrator di dominio. (Un solo processo può essere definito per ciascun orchestrator).

   **Server di posta IMAP**

   Specifica il nome host o l'indirizzo IP del server di posta elettronica che riceve i messaggi di posta elettronica in arrivo. Nella cartella Posta in arrivo per l'account di posta elettronica configurato viene eseguita la ricerca di nuovi messaggi di posta elettronica. Questo server deve avere il protocollo IMAP abilitato. Il trigger di posta non supporta POP3.

   **Porta del server IMAP**

   Se la porta TCP predefinita per un server IMAP viene utilizzata, immettere 143. Se si utilizzata una porta non predefinita o si imposta la comunicazione protetta su una porta diversa, richiedere all'amministratore di sistema la porta corretta da immettere.

   **Nome utente**

   Specifica il nome utente con cui connettersi al server di posta in arrivo. Osservare i requisiti del server IMAP quando si determina se immettere l'indirizzo di posta elettronica completo o l'alias come nome utente. Il nome utente pamadmin@ca.com è un esempio di un indirizzo completo mentre pamadmin corrisponde all'alias.

   **Nota:** Microsoft Exchange Server accetta sia l'indirizzo di posta elettronica completo sia l'alias.

   **Password**

   Specifica la password associata al nome utente specificato.

   **Intervallo di elaborazione posta elettronica (secondi)**

   La frequenza rappresenta i secondi con cui CA Process Automation cerca nel server IMAP nuovi messaggi di posta elettronica in arrivo nell'account specificato. Il nome utente e la password specificano l'account.

   **Predefinito:**

   2

**Salvataggio di allegati di posta nel database**

Specifica se salvare gli allegati dei messaggi di posta elettronica che attivano processi di CA Process Automation nel database.

- Opzione selezionata: CA Process Automation salva gli allegati dei messaggi di posta elettronica nel database di CA Process Automation e inserisce il set di dati del processo da avviare con le informazioni attinenti degli allegati.
- Cancellato: CA Process Automation non consente di salvare gli allegati dei messaggi di posta elettronica.

**Server di posta SMTP**

Specifica il nome del server per il server SMTP della posta in uscita. Quando un messaggio di posta elettronica di attivazione con contenuto XML valido viene ricevuto nell'account configurato del server di posta IMAP, viene restituito un messaggio di posta elettronica di riconoscimento. Questo viene restituito al mittente tramite il server SMTP in uscita.

**Porta del server SMTP**

Specifica la porta del server di posta in uscita.

**Predefinito:**

25

**Usare connessione SMTP protetta**

Specifica se procedere con l'elaborazione su una connessione protetta al server di posta SMTP.

- **Opzione selezionata**: il server di posta consente una connessione protetta al server di posta SMTP.
- **Opzione deselezionata**: il server di posta non consente una connessione protetta.

**Predefinito:**

Opzione deselezionata

4. Fare clic su Salva e chiudi.
5. Fare clic su Salva.
6. Selezionare Dominio e fare clic su Sblocca.

# Configurazione delle proprietà di trigger di SNMP a livello di dominio

Un amministratore con diritti Amministratore di dominio può configurare le proprietà di trigger SNMP a livello di dominio. Quando ereditate, le proprietà di trigger di SNMP abilitano processi da attivare dopo la ricezione di una trap di SNMP.

Prima di iniziare la configurazione delle proprietà di trigger SNMP, assicurarsi che la porta 162 sia accessibile a CA Process Automation. Modificare la porta di ascolto trap SNMP nei file di proprietà di CA Process Automation se si utilizza una porta alternativa.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione, selezionare Dominio e fare clic su Blocca.
2. Fare clic sulla scheda Trigger, fare clic con il pulsante destro del mouse su Trigger SNMP, quindi fare clic su Modifica.
3. Fare clic su Aggiungi parametro.
4. Nella finestra Trigger SNMP, completare i campi filtri Filtro trap se necessario.

5. Verificare che i dati immessi siano validi.

   Il filtro di esempio seguente accetta trap SNMP da qualsiasi host dotato delle caratteristiche seguenti:

   - Un indirizzo IP compreso tra 138.42.7.1 e 138.42.7.254 con un OID che inizia con 1.3.6.1.4.1.[x.x.x.x.x]
   - Almeno un valore di payload che corrisponde alla stringa letterale Test Payload for trigger.

   Quando il prodotto riceve una trap SNMP che corrisponde a questi criteri, attiva il processo RunProcess1 nel percorso /Test.

6. Fare clic sui pulsanti Sposta su e Sposta giù per ordinare l'elenco in base alla precedenza. Ciascun filtro ha la precedenza sui filtri elencati di seguito.

7. Fare clic su Salva.
8. Selezionare Dominio e fare clic su Sblocca.

**Ulteriori informazioni:**

Modifica della porta di ascolto trap SNMP (a pagina 336)

# Modifica della porta di ascolto trap SNMP

Per impostazione predefinita, CA Process Automation rileva sulla porta 162 per le trap di SNMP progettate per avviare processi di CA Process Automation. Se si chiude la porta 162 in corrispondenza del proprio sito e si configura una porta alternativa, modificare la configurazione di CA Process Automation per questa porta nel file OasisConfig.properties. Riavviare quindi il servizio Orchestrator.

È possibile modificare la porta su cui CA Process Automation rileva le trap SNMP.

**Attenersi alla procedura seguente:**

1. Accedere al server sul quale è configurato l'orchestrator di dominio.
2. Individuare la seguente cartella o directory:

   *install_dir*/server/c2o/.config/
3. Aprire il file OasisConfig.properties.
4. Modificare il valore nella seguente riga da 162 al numero di porta utilizzato per le trap SNMP.

   ```
   oasis.snmptrigger.service.port=162
   ```
5. Salvare il file.
6. Riavviare il servizio Orchestrator.
   a. Interrompere l'orchestrator (a pagina 196).
   b. Avviare l'orchestrator (a pagina 197).

   Appena il servizio si riavvia, CA Process Automation inizia a rilevare sulla porta configurata. CA Process Automation rileva i nuovi trap SNMP che soddisfano i criteri configurati nel trigger SNMP.

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

# Capitolo 14: Gestisci risorse utente

È possibile gestire risorse per utenti, orchestrator e agenti dal riquadro Gestisci risorse utente della scheda Configurazione.

Il riquadro Gestisci risorse utente contiene tre cartelle sotto Repository:

- Risorse agente
- Risorse orchestrator
- Risorse utente, che include la cartella secondaria, VBS_Resources.

  **Nota:** è possibile aggiungere cartelle secondarie solamente nella cartella Risorse utente.

Gli utenti a cui vengono concesse le autorizzazioni Configuration_User_Resources per la norma Browser di configurazione di CA EEM possono gestire le risorse nella cartella Risorse utente. Tuttavia, solo gli utenti a cui sono concesse anche le autorizzazioni Domain_Administrator delle norme di dominio possono accedere alle cartelle Risorse orchestrator e Risorse agente. I membri del gruppo predefinito PAMAdmins godono di entrambe autorizzazioni.

Questa sezione contiene i seguenti argomenti:

# Informazioni sulla gestione delle risorse degli utenti

La Gestione risorse richiede autorizzazioni specifiche per varie attività. Gli utenti appartenenti al gruppo predefinito PAMAdmins (il gruppo con diritti di accesso completi) possono eseguire qualsiasi attività di gestione delle risorse.

Gli utenti in gruppi personalizzati che dispongono di norme personalizzate devono disporre dei diritti di accesso di base, nonché una o entrambe delle seguenti autorizzazioni:

**Norma di ambiente PAM40: Environment_Configuration_Admin (Amministratore di configurazione)**

Gli utenti che dispongono delle autorizzazioni Environment_Configuration_Admin (Amministratore di configurazione) possono caricare, modificare o eliminare qualsiasi tipo di file nella cartella Risorse utente. Ad esempio:

- Un file di tipo jar da utilizzare con l'operatore Richiama Java
- Uno script da utilizzare con l'operatore Esegui script
- Un'immagine

**Norma di dominio PAM40: Domain_Admin (Amministratore)**

Gli utenti con autorizzazioni Domain_Admin (Amministratore) possono eseguire le seguenti attività:

- Aggiungere risorse alla cartella Risorse orchestrator o alla cartella Risorse agente.
- Modificare il contenuto di una risorsa e aggiungerlo nuovamente, nonché aggiornare i campi descrittivi.
- Eliminare una Risorsa orchestrator caricata precedentemente o una Risorsa agente.

**Nota:** le procedure per la modifica e l'eliminazione delle Risorse orchestrator e delle Risorse agente sono simili alle procedure per la modifica e l'eliminazione delle Risorse utente.

Le differenze fra Risorse utente e Risorse agente o Risorse orchestrator sono le seguenti:

**Risorse utente**

- Dopo un riavvio, l'agente o la variabile classpath dell'orchestrator non includeranno le risorse caricate sulla cartella Risorse utente.
- È possibile creare cartelle secondarie dentro la cartella Risorse utente.
- Non sono necessari i diritti Domain_Admin (amministratore).

**Risorse agente e Risorse orchestrator**

- Dopo un riavvio, l'agente o la variabile classpath dell'orchestrator includeranno risorse caricate nelle cartelle Risorse agente e Risorse orchestrator.

- Non è possibile creare cartelle secondarie nelle cartelle Risorse agente e Risorse orchestrator.
- È necessario disporre dei diritti Domain_Admin (amministratore).

# Distribuzione dei driver JDBC per gli operatori di database

È possibile installare i driver JDBC per gli operatori di database durante o dopo l'installazione di CA Process Automation. Solamente i processi con operatori di database richiedono un driver JDBC.

Durante l'installazione, i driver JDBC caricati nell'installazione del software di terze parti sono visualizzati, ma non selezionati. È possibile selezionare i driver JDBC per MySQL, Microsoft SQL Server e Oracle. Inoltre, è possibile aggiungere altri file JAR copiati in una directory locale.

Dopo l'installazione, è possibile caricare i file JAR che contengono driver JDBC per gli operatori Database utilizzando il riquadro Gestisci risorse utente nella scheda Configurazione. CA Process Automation effettua la distribuzione dei file JAR caricati su orchestrator o agenti, a seconda della cartella selezionata durante il caricamento. Per ulteriori informazioni, consultare i seguenti argomenti:

- Caricamento Risorse orchestrator (a pagina 339).
- Caricamento Risorse agente (a pagina 341).

# Caricamento Risorse orchestrator

Dopo l'installazione, la cartella Risorse orchestrator visualizza solamente i file jar di JDBC che sono stati aggiunti durante l'installazione. Dopo aver utilizzato il riquadro Gestisci risorse utente per l'aggiornamento della cartella Risorse orchestrator, tale cartella conterrà i file jar aggiornati.

È possibile caricare un file jar nella cartella Risorse orchestrator dell'Orchestrator di dominio. Quando si riavvia l'orchestrator di dominio, CA Process Automation effettua la distribuzione del file all'orchestrator di dominio. L'orchestrator di dominio esegue la duplicazione del file all'intervallo di mirroring configurato, dopo il quale verranno riavviati gli altri orchestrator. Quando gli orchestrator vengono riavviati, il file duplicato può essere utilizzato.

**Nota:** Il mirroring si applica a tutti gli orchestrator nel dominio. Per gli orchestrator in cluster, il mirroring si applica a tutti i nodi in ciascun cluster.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic sul riquadro Gestisci risorse utente ed espandere la cartella Repository.

3. Selezionare la cartella Risorse orchestrator.
4. Fare clic su Nuovo.

   Viene visualizzato il riquadro Aggiungi nuova risorsa: "Senza titolo".
5. Immettere i dettagli di caricamento richiesti nei seguenti campi:
   a. Immettere il nome della risorsa nel campo Nome risorsa.

      L'esempio seguente mostra un metodo semplice per specificare il nome della risorsa in caso di caricamento di un driver JDBC:

      `Driver` *`nome_database`*

      ***database_name***

      Definisce il nome del RDBMS. Ad esempio, driver Oracle, driver MySQL o driver Sybase.
   b. Fare clic su Sfoglia, accedere alla posizione utilizzata per il salvataggio del file JAR e selezionare il file di destinazione. Viene così compilato il campo File risorsa.
   c. Selezionare un nome di modulo definito dall'utente dall'elenco a discesa Nome modulo.
   d. (Facoltativo) Immettere la descrizione della soluzione nel campo Descrizione risorsa.
6. Verificare la voce, quindi fare clic su Salva.

   Viene visualizzata una riga con la voce.

   | Nome | Tipo di file | Percorso file | Modulo |
   |---|---|---|---|
   | Sybase Driver | jar | .c2oserverresources/lib/jconn2.jar | Sybase Driver |

   CA Process Automation esegue la copia della risorsa caricata sui seguenti percorsi:

   *`install_dir`*`/server/c2o/ext-lib`

   *`install_dir`*`/server/c2o/.c2orepository/.c2oserverresources/lib`

   ***install_dir***

   Definisce la directory del server su cui è stato installato l'orchestrator di dominio.
7. Riavviare l'orchestrator di dominio. (Arrestare l'orchestrator di dominio (a pagina 196), quindi avviare nuovamente l'orchestrator di dominio (a pagina 197).)

   Quando l'orchestrator di dominio viene riavviato, tutti i file jar caricati vengono distribuiti nelle Risorse orchestrator di dominio. Ciò significa che CA Process Automation posiziona i file jar nella variabile classpath dell'orchestrator di dominio.
8. Dopo il mirroring, riavviare gli altri orchestrator.

   Il sistema effettua la distribuzione di tutti i file jar caricati sugli orchestrator. Il sistema posiziona i file jar nelle variabili classpath degli orchestrator.

   **Nota:** Per gli orchestrator in cluster, riavviare ciascun nodo.

# Caricamento Risorse agente

Gli utenti con autorizzazioni di amministratore di dominio possono caricare risorse nella cartella Risorse agente sull'orchestrator di dominio. La risorsa caricata può essere un file jar, ad esempio un driver JDBC. Le risorse agente caricate vengono copiate nell'intervallo di mirroring configurato. Dopo il mirroring, gli agenti vanno riavviati. Gli agenti riavviati possono utilizzare le risorse di agente caricate.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA Process Automation (a pagina 18).
2. Fare clic sulla scheda Configurazione.
3. Fare clic sul riquadro Gestisci risorse utente ed espandere la cartella Repository.
4. Selezionare la cartella Risorse agente e fare clic su Nuovo.

   Viene visualizzato il riquadro Aggiungi nuova risorsa: "Senza titolo".
5. Fornire i dettagli di caricamento, utilizzando, se necessario, le seguenti descrizioni dei campi.
   a. Immettere il nome della risorsa nel campo Nome risorsa.

      Se si sta caricando un driver JDBC, digitare Driver *nome_database* in cui *nome_database* corrisponde al sistema RDBMS. Ad esempio, driver Oracle, driver MySQL o driver Sybase.
   b. Fare clic su Sfoglia, accedere alla posizione utilizzata per il salvataggio del file JAR e selezionare il file di destinazione.

      Il campo File risorsa viene compilato con il file e il relativo percorso.
   c. (Facoltativo) Selezionare un nome di modulo definito dall'utente dall'elenco a discesa Nome modulo.
   d. (Facoltativo) Immettere una descrizione inerente nel campo Descrizione risorsa.
6. Verificare la voce. Quindi, fare clic su Salva.

   Viene visualizzata una riga con la voce.

   CA Process Automation copia le risorse caricate, ad esempio un driver JDBC, nel seguente percorso, dove *install_dir* è la directory sul server in cui è stato installato l'orchestrator di dominio.

   ```
   install_dir/server/c2o/.c2orepository/.c2oagentresources/lib/drivers/jars
   ```
7. Al termine del processo di mirroring, riavviare gli agenti in cui sono necessari i file jar caricati. I file jar vengono posti nel classpath degli agenti riavviati.

   **Nota:** per informazioni sul riavvio degli agenti, consultare Avvio o arresto di un agente.

# Caricamento Risorse utente

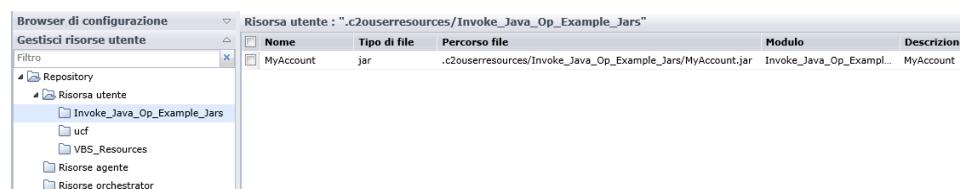
Il caricamento richiede di creare una cartella nella cartella Risorse utente e raggiungere la risorsa da caricare. CA Process Automation aggiunge la risorsa alla struttura ad albero risorse utente e carica la risorsa.

Consultare le seguenti procedure:

- Aggiunta di una risorsa a Risorse utente (a pagina 342).
- Eliminazione di una risorsa da Risorse utente (a pagina 343).
- Modifica di una risorsa in Risorse utente (a pagina 344).

**Nota:** per modificare il percorso delle risorse, eliminare la risorsa e aggiungerla di nuovo sotto un percorso differente.

## Risorsa per eseguire l'esempio di operatore Richiama Java

Il processo di installazione aggiunge una risorsa alla cartella Risorsa utente in Repository nel riquadro Gestisci risorse utente della scheda Configurazione. Il file JAR, MyAccount.jar, si trova nella cartella Invoke_Java_Op_Example_jars. È possibile utilizzare il file MyAccount.jar per eseguire l'esempio di Java fornito nel campo Metodo principale richiesto dell'operatore Richiama Java.

## Aggiunta di una risorsa alle Risorse utente

Gli utenti con autorizzazioni a livello di amministrazione possono aggiungere gli script alla cartella delle risorse utente nel repository globale. Il prodotto esegue il mirroring delle risorse utente caricate nell'intervallo di mirroring configurato su altri orchestrator e agenti nel dominio. Gli orchestrator e gli agenti possono accedere alle risorse dell'utente come riferimento.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic sul riquadro Gestisci risorse utente.
3. Espandere la cartella Repository, quindi espandere la cartella Risorsa utente.
4. Selezionare la cartella Risorsa utente o una sottocartella e fare clic su Nuovo.

5. Compilare i campi nel riquadro Aggiungi nuova risorsa se necessario.
6. Verificare le voci, quindi fare clic su Salva.

   L'elenco nel riquadro Risorsa utente visualizza nome, tipo, percorso, modulo e descrizione del file caricato.

Il prodotto copia le risorse dell'utente caricate nel percorso seguente:

`install_dir/server/c2o/.c2orepository/.c2ouserresources/...`

***install_dir***

Definisce la directory del server su cui è stato installato l'orchestrator di dominio.

Se necessario, il prodotto crea sottocartelle per gestire il percorso dalla cartella Risorse utente nella risorsa.

**Ulteriori informazioni:**

Caricamento dei descrittori di Catalyst (a pagina 279)

## Eliminazione di una risorsa dalle Risorse utente

È possibile eliminare una risorsa, come un file di script o un file jar, aggiunta alla cartella Risorse utente.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic sul riquadro Gestisci risorse utente.
3. Espandere la cartella Repository. Espandere la cartella Risorse utente.
4. Fare clic sulla cartella contenente la risorsa.
5. Fare clic sulla riga che visualizza il nome della risorsa da eliminare, quindi fare clic su Elimina.

**Nota:** quando viene eliminata l'ultima risorsa da una cartella secondaria di Risorse utente, viene eliminata anche la cartella secondaria.

## Modifica di una risorsa in Risorse utente

È possibile modificare una risorsa nei modi seguenti:

- È possibile modificare il testo in qualsiasi campo visualizzato, fatta eccezione per il campo Percorso della risorsa. È possibile eseguire l'azione se viene selezionata l'opzione Sostituisci file.
- È possibile caricare una risorsa modificata, come un file di script o un file jar, aggiunta precedentemente alle Risorse utente. È possibile eseguire l'azione se si seleziona Sostituisci file.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Fare clic sul riquadro Gestisci risorse utente.
3. Espandere la cartella Repository, quindi espandere la cartella Risorse utente.
4. Fare clic sulla cartella contenente la risorsa.
5. Fare clic con il tasto destro del mouse sulla riga che visualizza il nome della risorsa da modificare, quindi selezionare Modifica.

   Viene visualizzata la pagina Risorsa.
6. (Facoltativo) Modificare le informazioni relative alla risorsa. È possibile modificare i campi seguenti:
   - Nome risorsa
   - Nome modulo
   - Descrizione risorsa
7. Impostare la casella di controllo Sostituisci file nella seguente maniera:
   - Se le *uniche* modifiche apportate alle risorse sono i campi aggiornati della pagina Risorsa, deselezionare la casella di controllo Sostituisci file e fare clic su Salva.
   - Se la copia locale del File risorsa è stata aggiornata e si desidera caricare gli aggiornamenti:
     a. Selezionare Sostituisci file.
     b. Fare clic su Sfoglia.
     c. Accedere al file di aggiornato e fare clic su Apri.
     d. Fare clic su Salva.

   La cartella Risorse utente conterrà il file aggiornato. La pagina Risorse include il testo per qualsiasi campo modificato.

# Capitolo 15: Controllo delle azioni dell'utente

CA Process Automation fornisce audit trail per tenere traccia e registrare le attività per gli oggetti di configurazione (dominio, ambienti, agenti e orchestrator) e gli oggetti di libreria (cartelle e oggetti di automazione). L'amministratore di dominio può visualizzare l'audit trail per il dominio. Un amministratore della configurazione dell'ambiente può visualizzare l'audit trail per un ambiente. Un utente finale con autorizzazione Utente di ambiente può visualizzare l'audit trail per un oggetto.

Questa sezione contiene i seguenti argomenti:



## Visualizzazione dell'audit trail per il dominio

Gli amministratori possono visualizzare l'audit trail del dominio.

L'audit trail del dominio controlla le azioni seguenti:

- Dominio bloccato e sbloccato.
- Proprietà di dominio modificata.
- Orchestrator di dominio modificato.
- Ambiente creato, eliminato, bloccato, sbloccato o rinominato.
- Orchestrator aggiunto, eliminato o rinominato.
- Agente aggiunto, eliminato o rinominato.
- Il riferimento agente era stato assegnato al touchpoint "nome-touchpoint".

L'esempio seguente mostra l'audit trail relativo all'assegnazione di un touchpoint a un agente. Due delle colonne sono nascoste.

**Attenersi alla procedura seguente:**

1. Selezionare la scheda Configurazione.
2. Nel riquadro Browser di configurazione, selezionare il nodo Dominio.
3. Nel riquadro Contenuti, fare clic sulla scheda Audit trail.

   La scheda Audit trail visualizza le informazioni seguenti per tutti i record:

   - Nome dell'oggetto
   - Ultimo aggiornamento
   - Nome utente
   - Tipo di azione
   - Descrizione

4. (Facoltativo) Per ordinare gli audit trail in base a una colonna specifica, selezionare Ordinamento crescente o Ordinamento decrescente dall'elenco a discesa della colonna di destinazione.

   Ad esempio, per rivedere un utente specifico, selezionare un'opzione di ordinamento dall'elenco a discesa della colonna Nome utente, quindi scorrere fino al record appropriato.

5. (Facoltativo) Per modificare il numero di record visualizzati dal prodotto in una pagina, selezionare un valore dall'elenco a discesa Righe per pagina.
6. Analizzare i record dell'audit trail.

   Se i record di audit comprendono più pagine, utilizzare i pulsanti di navigazione sulla barra degli strumenti per visualizzare la prima pagina, quella precedente, quella successiva o l'ultima.

# Visualizzazione dell'audit trail per un ambiente

Con i diritti di accesso di amministratore di configurazione, è possibile visualizzare l'audit trail relativo all'ambiente.

L'audit trail di un ambiente controlla le azioni seguenti:

- Ambiente bloccato o non bloccato. Proprietà dell'ambiente modificata.
- Ambiente creato o eliminato.
- Ambiente o oggetto nell'ambiente rinominato.
- Touchpoint aggiunto, eliminato o rinominato.
- Gruppo touchpoint aggiunto o eliminato.
- Gruppo host aggiunto o eliminato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Nel riquadro Browser di configurazione, espandere il nodo Dominio e selezionare l'ambiente da rivedere (ad esempio, Ambiente predefinito).
3. Nel riquadro Contenuti, fare clic sulla scheda Audit trail.

   La scheda Audit trail visualizza le informazioni seguenti per tutti i record:

   - Nome dell'oggetto
   - Ultimo aggiornamento
   - Nome utente
   - Tipo di azione
   - Descrizione
4. (Facoltativo) Per ordinare gli audit trail in base a una colonna specifica, selezionare Ordinamento crescente o Ordinamento decrescente dall'elenco a discesa della colonna di destinazione.

   Ad esempio, per rivedere un utente specifico, selezionare un'opzione di ordinamento dall'elenco a discesa della colonna Nome utente, quindi scorrere fino al record appropriato.
5. (Facoltativo) Per modificare il numero di record visualizzati dal prodotto in una pagina, selezionare un valore dall'elenco a discesa Righe per pagina.
6. Analizzare i record dell'audit trail.

   Se i record di audit comprendono più pagine, utilizzare i pulsanti di navigazione sulla barra degli strumenti per visualizzare la prima pagina, quella precedente, quella successiva o l'ultima.

## Visualizzazione dell'audit trail per un orchestrator

Con le autorizzazioni di lettura per un oggetto di configurazione, è possibile visualizzare l'audit trail associato. La visualizzazione dell'audit trail per gli oggetti di configurazione richiede i diritti di accesso che includono Utente di ambiente e Visualizza browser di configurazione.

L'audit trail di un orchestrator controlla le azioni seguenti:

- Orchestrator bloccato o non bloccato.
- Proprietà di orchestrator modificata.
- Orchestrator in quarantena o non in quarantena.
- Orchestrator mappato su un touchpoint o non mappato da un touchpoint.
- Orchestrator rinominato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Nel riquadro Browser di configurazione, espandere il nodo Orchestrator e selezionare l'orchestrator di destinazione.
3. Nel riquadro Contenuti, fare clic sulla scheda Audit trail.

   La scheda Audit trail visualizza le informazioni seguenti per tutti i record:

   - Nome dell'oggetto
   - Ultimo aggiornamento
   - Nome utente
   - Tipo di azione
   - Descrizione

4. (Facoltativo) Per ordinare gli audit trail in base a una colonna specifica, selezionare Ordinamento crescente o Ordinamento decrescente dall'elenco a discesa della colonna di destinazione.

   Ad esempio, per rivedere un utente specifico, selezionare un'opzione di ordinamento dall'elenco a discesa della colonna Nome utente, quindi scorrere fino al record appropriato.

5. (Facoltativo) Per modificare il numero di record visualizzati dal prodotto in una pagina, selezionare un valore dall'elenco a discesa Righe per pagina.
6. Analizzare i record dell'audit trail.

   Se i record di audit comprendono più pagine, utilizzare i pulsanti di navigazione sulla barra degli strumenti per visualizzare la prima pagina, quella precedente, quella successiva o l'ultima.

# Visualizzazione dell'audit trail per un agente

Con le autorizzazioni di lettura per un oggetto di configurazione, è possibile visualizzare l'audit trail associato. La visualizzazione dell'audit trail degli oggetti di configurazione richiede i diritti di accesso di CA EEM che includono Utente di ambiente e Visualizza browser di configurazione.

L'audit trail di un agente controlla le azioni seguenti:

- Categoria operatore abilitata nella scheda Moduli e modifica di un valore configurato.
- Agente in quarantena o non in quarantena.
- Agente bloccato o non bloccato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Nel riquadro Browser di configurazione, espandere il nodo Agenti e selezionare l'agente di destinazione.
3. Nel riquadro Contenuti, fare clic sulla scheda Audit trail.

   La scheda Audit trail visualizza le informazioni seguenti per tutti i record:

   - Nome dell'oggetto
   - Ultimo aggiornamento
   - Nome utente
   - Tipo di azione
   - Descrizione

4. (Facoltativo) Per ordinare gli audit trail in base a una colonna specifica, selezionare Ordinamento crescente o Ordinamento decrescente dall'elenco a discesa della colonna di destinazione.

   Ad esempio, per rivedere un utente specifico, selezionare un'opzione di ordinamento dall'elenco a discesa della colonna Nome utente, quindi scorrere fino al record appropriato.

5. (Facoltativo) Per modificare il numero di record visualizzati dal prodotto in una pagina, selezionare un valore dall'elenco a discesa Righe per pagina.
6. Analizzare i record dell'audit trail.

   Se i record di audit comprendono più pagine, utilizzare i pulsanti di navigazione sulla barra degli strumenti per visualizzare la prima pagina, quella precedente, quella successiva o l'ultima.

# Visualizzazione dell'audit trail per un touchpoint, gruppo di touchpoint, o gruppo host

Con le autorizzazioni di lettura per un oggetto di configurazione, è possibile visualizzare l'audit trail associato. La visualizzazione dell'audit trail per gli oggetti di configurazione richiede i diritti di accesso che includono Utente di ambiente e Visualizza browser di configurazione.

Gli audit trail di un touchpoint, un gruppo touchpoint e un gruppo host controllano le azioni seguenti:

- Touchpoint creato
- Agente assegnato a un touchpoint
- Gruppo touchpoint creato
- Touchpoint aggiunto a un gruppo
- Gruppo touchpoint rinominato
- Gruppo host creato

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Configurazione.
2. Nel riquadro Browser di configurazione, espandere il nodo Dominio. Quindi, espandere il nodo Ambiente che contiene il touchpoint di destinazione, il gruppo touchpoint o il gruppo host.
3. Espandere il nodo appropriato (Tutti i touchpoint, Tutti i gruppi touchpoint o Tutti i gruppi host) e selezionare il touchpoint di destinazione, il gruppo touchpoint o il gruppo host.
4. Nel riquadro Contenuti, fare clic sulla scheda Audit trail.

   La scheda Audit trail visualizza le informazioni seguenti per tutti i record:

   - Nome dell'oggetto
   - Ultimo aggiornamento
   - Nome utente
   - Tipo di azione
   - Descrizione
5. (Facoltativo) Per ordinare gli audit trail in base a una colonna specifica, selezionare Ordinamento crescente o Ordinamento decrescente dall'elenco a discesa della colonna di destinazione.

   Ad esempio, per rivedere un utente specifico, selezionare un'opzione di ordinamento dall'elenco a discesa della colonna Nome utente, quindi scorrere fino al record appropriato.

6. (Facoltativo) Per modificare il numero di record visualizzati dal prodotto in una pagina, selezionare un valore dall'elenco a discesa Righe per pagina.
7. Analizzare i record dell'audit trail.

   Se i record di audit comprendono più pagine, utilizzare i pulsanti di navigazione sulla barra degli strumenti per visualizzare la prima pagina, quella precedente, quella successiva o l'ultima.

# Visualizzazione dell'audit trail per una cartella della libreria

Gli amministratori possono visualizzare l'audit trail per qualsiasi cartella selezionata nella libreria. Il prodotto registra le azioni seguenti per le cartelle in una libreria:

- Creato
- Rinominato
- Eliminato
- Creazione o eliminazione di un oggetto di automazione
- Recupero di un oggetto di automazione o di una cartella dal cestino
- Modifica delle autorizzazioni nella cartella, inclusi i collegamenti a ad ACL nuovi e precedenti.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria e selezionare un orchestrator dall'elenco a discesa Orchestrator.
2. Accedere alla cartella che contiene la cartella da rivedere.
3. Nel riquadro Sommario, fare clic con il pulsante destro del mouse sulla cartella da rivedere, quindi selezionare Proprietà.
4. Nel riquadro Proprietà, fare clic sulla scheda Audit trail.

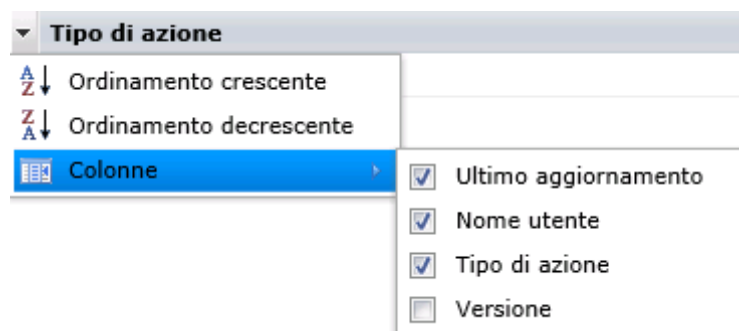
   La scheda Audit trail visualizza le informazioni seguenti per tutti i record:

   - Ultimo aggiornamento
   - Nome utente
   - Tipo di azione
5. (Facoltativo) Per ordinare gli audit trail in base a una colonna specifica, selezionare Ordinamento crescente o Ordinamento decrescente dall'elenco a discesa della colonna di destinazione.

6. (Facoltativo) Definire quali colonne deve visualizzare il prodotto:

   a. Selezionare Colonne dall'elenco a discesa in qualsiasi intestazione di colonna.

   b. Deselezionare (nascondere) o selezionare (visualizzare) le caselle di controllo delle colonne, se necessario.

   Ad esempio, per visualizzare la colonna Versione, selezionare la casella di controllo Versione dal menu di Colonne.

7. Analizzare i record dell'audit trail.

# Visualizzazione dell'audit trail per un oggetto di automazione aperto

Gli amministratori possono visualizzare l'audit trail di un oggetto di automazione aperto. Il prodotto registra le azioni seguenti per gli oggetti di automazione:

- Crea
- Elimina
- Archivia ed Estrai
- Rinomina
- Esporta e Importa
- Modifica delle autorizzazioni per gli oggetti di automazione, inclusi i collegamenti ad ACL nuovi e precedenti.
- Recupero di un oggetto di automazione dal cestino
- Modifica della versione designata corrente
- Creazione o aggiornamento della versione di rilascio
- Aggiunta di una proprietà della versione di rilascio
- Aggiornamento di un oggetto di automazione (ad esempio una pianificazione) senza estrazione
- Operazione per rendere un oggetto Operatore personalizzato disponibile o non disponibile
- Attivazione o disattivazione di una pianificazione

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria e selezionare un orchestrator dall'elenco a discesa Orchestrator.
2. Accedere alla cartella che contiene l'istanza dell'oggetto di automazione da rivedere.
3. Nel riquadro Sommario, fare clic con il pulsante destro del mouse sull'istanza dell'oggetto di automazione da controllare, quindi selezionare Proprietà.
4. Nel riquadro Proprietà, fare clic sulla scheda Audit trail.

   La scheda Audit trail visualizza le informazioni seguenti per tutti i record:

   - Ultimo aggiornamento
   - Nome utente
   - Tipo di azione

   **Nota:** È disponibile anche la colonna Versione, ma non viene visualizzata per impostazione predefinita. Per ulteriori informazioni, consultare il passaggio 5.

5. (Facoltativo) Per ordinare gli audit trail in base a una colonna specifica, selezionare Ordinamento crescente o Ordinamento decrescente dall'elenco a discesa della colonna di destinazione.

   Ad esempio, per rivedere un utente specifico, selezionare un'opzione di ordinamento dall'elenco a discesa della colonna Nome utente, quindi scorrere fino al record appropriato.

6. (Facoltativo) Definire quali colonne deve visualizzare il prodotto:

   a. Selezionare Colonne da un elenco a discesa della colonna.

   b. Deselezionare (nascondere) o selezionare (visualizzare) le caselle di controllo delle colonne, se necessario.

   Ad esempio, per visualizzare la colonna Versione, selezionare la casella di controllo Versione dal menu di Colonne.

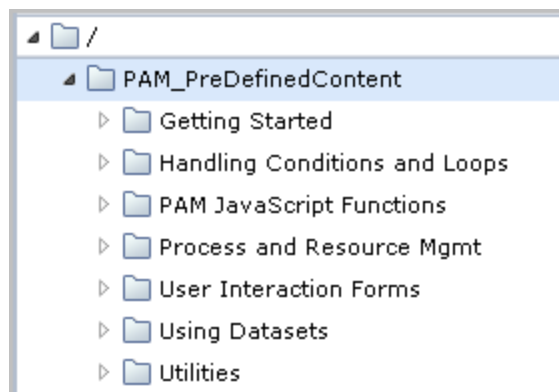
7. Analizzare i record dell'audit trail.

# Capitolo 16: Amministrazione degli oggetti di libreria

Questa sezione contiene i seguenti argomenti:



## Creazione e gestione di cartelle

La libreria di un orchestrator di dominio di CA Process Automation appena installato non contiene cartelle nel riquadro di navigazione della scheda Libreria. L'installazione del contenuto predefinito dalla pagina iniziale permette di creare le cartelle nella libreria per il contenuto predefinito.

Generalmente, un amministratore configura la struttura di cartella in base ai contenuti creati dai responsabili di progettazione. I responsabili di progettazione salvano tutti gli oggetti di automazione nelle cartelle di libreria. Per impostazione predefinita, possono creare cartelle i membri del gruppo dei responsabili di progettazione.

**Nota:** per un'applicazione di CA Process Automation aggiornata, viene eseguita la migrazione di tutte le cartelle nella struttura precedente con i relativi contenuti.

# Configurazione delle cartelle per la progettazione

È possibile utilizzare il processo seguente per configurare le cartelle:

1. Pianificazione della struttura di cartella (a pagina 356).
2. Creazione di cartelle (a pagina 358).
3. Concessione del diritto di accesso alle cartelle (a pagina 358).

## Pianificazione della struttura di cartella

Una delle prime decisioni come nuovo amministratore di CA Process Automation riguarda l'organizzazione e l'uso delle cartelle nella scheda Libreria. È possibile aumentare la profondità della struttura di cartella in base alle proprie esigenze.

Per facilitare l'attività preparatoria ai fini dell'esportazione, configurare una struttura di cartella analoga a quella descritta prima di iniziare con il lavoro di progettazione. A livello di directory principale della libreria, creare una cartella per ogni processo che si intende automatizzare. In ciascuna cartella a livello di processo, creare una cartella a livello di rilascio secondo le convenzioni di denominazione per la prima versione di rilascio. In caso di aggiornamenti per un processo, è possibile aggiungere nuove cartelle per le versioni di rilascio successive.

```
/ (cartella principale)
Processo automatizzato 1
   Versione di rilascio 1
   Versione di rilascio 2
Processo automatizzato 2
   Versione di rilascio 1
   Versione di rilascio 2
```

Quando viene distribuita la prima versione di rilascio del primo processo automatizzato, si esporta la cartella della versione di rilascio con tutti gli oggetti contenuti nel rilascio.

Considerare gli approcci seguenti per la creazione di una struttura di cartella:

- Creare la struttura di esportazione dall'inizio e utilizzare la cartella della versione di rilascio come cartella di lavoro. I responsabili di progettazione dei contenuti creano, aggiornano e testano gli oggetti all'interno della cartella della versione di rilascio o in una delle cartelle secondarie. Qualunque struttura di cartella creata qui ed esportata viene riprodotta nell'ambiente di produzione dopo l'importazione.
- Creare le cartelle di lavoro. Quando la prima versione di rilascio di un processo è pronta per la distribuzione, creare la cartella di esportazione e popolarla con gli oggetti compresi nella versione di rilascio.
- Approccio misto. Creare la struttura di esportazione e utilizzare la cartella di esportazione per la prossima versione di rilascio come cartella di lavoro, mantenendo gli oggetti condivisi tra i processi in una cartella diversa a livello di directory principale. Ad esempio, più processi possono condividere oggetti del set di dati e sottoprocessi specifici. È possibile condividere i calendari nelle pianificazioni. È possibile condividere le pianificazioni globali. Quindi, durante la preparazione per l'esportazione, copiare gli oggetti richiesti dalla cartella degli oggetti condivisi a quella di esportazione.

**Nota:** Se si esporta una cartella con percorsi assoluti, nell'ambiente di produzione viene replicata la struttura completa della cartella di esportazione una volta importati i contenuti.

## Creazione di cartelle

Le cartelle vengono create nel riquadro sinistro della scheda Libreria. Il riquadro sinistro è il riquadro di navigazione per la libreria. Una cartella contiene il contenuto progettato dai responsabili di progettazione a partire dagli oggetti di automazione. Tutti gli oggetti che supportano un processo automatizzato specifico devono trovarsi nella stessa cartella o struttura di cartella per l'esportazione. È utile creare una cartella a livello di directory principale per ciascun progetto.

In una cartella a livello di processo è possibile creare cartelle secondarie. In fase di esportazione, la cartella che si esporta come pacchetto di contenuto non può contenere oggetti inutilizzati oppure obsoleti. La struttura di cartella definita per un progetto nell'ambiente di progettazione viene replicata nell'ambiente di produzione dopo l'importazione.

**Attenersi alla procedura seguente:**

1. Decidere a quale livello si desidera la cartella.

   È possibile creare una cartella sotto il nodo principale o una cartella esistente.

2. Fare clic con il pulsante destro del mouse sul nodo principale della cartella e selezionare Nuovo oggetto, Cartella.

   Il percorso di cartella viene visualizzato nel riquadro principale con un campo per il nome. Il nome predefinito visualizzato è Cartella.

3. Fare clic sul campo Nome, eliminare il nome di cartella predefinito e immetterne un altro per questa nuova cartella.

## Concessione dei diritti di accesso alle cartelle

Gli amministratori, membri del gruppo PAMAdmins, dispongono dell'accesso a tutte le cartelle e ai relativi contenuti.

È possibile consentire l'accesso alla cartella agli utenti non amministratori nei modi seguenti:

- Impostare la titolarità della cartella (a pagina 359).

  L'utente che crea la cartella (o l'oggetto di automazione) è il primo titolare. Se tutte le cartelle vengono create dall'amministratore, l'opzione Imposta titolare consente di concedere l'accesso alla cartella agli utenti non amministratori.

- Creare una policy per ciascun responsabile di progettazione dei contenuti (a pagina 359).

  È possibile concedere l'accesso a cartelle specifiche ai responsabili di progettazione dei contenuti (membri di PAMUsers o di un gruppo personalizzato) che non dispongono dei diritti di amministratore del contenuto.

## Impostazione della titolarità della cartella

Solo un amministratore del contenuto o il titolare di cartella può modificare la titolarità di una cartella. Per impostazione predefinita, il creatore della cartella è il titolare. Il titolare dispone di autorizzazioni illimitate sulla cartella. L'amministratore del contenuto può creare una cartella e quindi trasferire la titolarità della cartella all'ID utente appropriato. Ad esempio, i responsabili di progettazione dei contenuti potrebbero avere cartelle proprie, ma la cartella utilizzata per esportare una versione di rilascio come pacchetto di contenuto potrebbe essere assegnata a un amministratore.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:ambiente* appropriato.
3. Selezionare una cartella.
4. Fare clic su Imposta titolare.
5. Immettere l'ID dell'utente da impostare come titolare e fare clic su Cerca.

   **Nota:** I risultati della ricerca includono tutti gli utenti con un ID utente o un nome utente che contiene la stringa immessa.
6. Selezionare l'utente dall'elenco visualizzato.
7. Fare clic su Salva e chiudi.

**Nota:** La titolarità di una cartella permette di accedere alla cartella, nonché di esportarla individualmente o come un pacchetto di contenuto. Con una policy di CA EEM, si ha un controllo maggiore sulle azioni che un responsabile di progettazione dei contenuti può eseguire su una cartella.

## Creazione di una norma per ciascun responsabile di progettazione dei contenuti

Una volta che la propria struttura di cartella è implementata e i responsabili di progettazione dei contenuti dispongono di account utente, è possibile concedere loro l'accesso alle cartelle. L'accesso alle cartelle specifica la cartella in cui un utente o il gruppo applicazioni può creare e controllare oggetti di automazione. Questa procedura presuppone che si assegni una cartella distinta a ciascun responsabile di progettazione dei contenuti e che queste cartelle si trovino direttamente sotto la cartella principale.

Una norma personalizzata in base all'oggetto consente di concedere l'accesso alla cartella agli utenti o gruppi specificati. I diritti di accesso disponibili per le cartelle includono Elenco, Lettura, Modifica, Elimina e Amministratore. Dopo aver creato la prima norma, è possibile utilizzarla come modello per la creazione di altre norme.

**Attenersi alla procedura seguente:**

1. Eseguire l'accesso a CA EEM (a pagina 45).
2. Fare clic sulla scheda di gestione delle norme di accesso.
3. Fare clic su Nuova norma di accesso per Oggetto.

   Viene visualizzata una nuova norma di accesso in cui il nome di classe risorsa è Oggetto.
4. Immettere un nome per questa norma che consente l'accesso alla cartella a un determinato responsabile di progettazione dei contenuti.
5. Fare clic sul collegamento Cerca identità, quindi fare clic su Cerca.
6. Selezionare il nome del responsabile di sviluppo dei contenuti e fare clic sulla freccia di destra.

   Il nome viene visualizzato nell'elenco Identità selezionate preceduto da [Utente].
7. Immettere il percorso e il nome della cartella creata per questo responsabile di progettazione dei contenuti nel campo Aggiungi risorsa e fare clic su Aggiungi risorsa.

   La voce immessa viene visualizzata nell'elenco Risorse
8. Selezionare ciascuna autorizzazione da concedere al responsabile di progettazione dei contenuti. Ad esempio, consentire tutte le azioni eccetto Object_Admin.
9. Fare clic su Salva.

   La norma salvata è simile a quella illustrata di seguito:

| Nome/Descrizione | ResourceClassName | Opzioni | Identità | Azioni | Risorse |
|---|---|---|---|---|---|
| Folder Access for Content Designer 1<br>Grants Content Designer 1 access to the /ContentDesigner1 folder | Object | Concessione esplicita | content designer 1 | Object_List<br>Object_Read<br>Object_Edit<br>Object_Delete | /ContentDesigner1 |

10. Verificare l'accesso.
    a. Accedere a CA Process Automation con le credenziali di questo utente.
    b. Verificare che l'unica cartella utilizzabile sia quella con i diritti di accesso concessi.
11. Creare una norma per ogni altro responsabile di progettazione dei contenuti in uno dei modi seguenti:
    - Ripetere i passaggi da 2 a 10.
    - Aprire la norma salvata, fare clic su Salva con nome, immettere un nuovo nome e modificare.

**Nota:** per concedere l'accesso di lettura per tutte le cartelle, creare una norma con l'oggetto a cui aggiungere tutti i responsabili di progettazione dei contenuti. Selezionare Object_List e Object_Read per la cartella principale.

## Gestione delle cartelle

Per gestire le cartelle, è possibile utilizzare una qualsiasi combinazione delle procedure seguenti:

- Eseguire il backup di tutte le cartelle e dei contenuti (a pagina 367).
- Eliminare una cartella (a pagina 368).
- Esportare una cartella (a pagina 363).
- Importare una cartella (a pagina 364).
- Spostare una cartella (a pagina 362).
- Cercare la struttura di cartella (a pagina 361).
- Visualizzare i contenuti di una cartella (a pagina 362).

**Note:**

- Consultare Preparazione dell'ambiente di produzione per un nuovo rilascio (a pagina 370) per maggiori informazioni sull'esportazione di una cartella come pacchetto di contenuto.
- Consultare Utilizzo del cestino (a pagina 387) per maggiori informazioni sull'eliminazione definitiva e il ripristino delle cartelle eliminate.

### Ricerca della struttura di cartella

È possibile eseguire una query per cercare le cartelle con un nome che inizia con la stringa o la stringa parziale specificata. Il campo di ricerca si trova nella parte superiore del riquadro sinistro nella scheda Libreria.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:environment* appropriato.
3. Immettere il nome o parte del nome per una cartella o insieme di cartelle nel campo di ricerca.
4. Esaminare l'elenco filtrato. Verificare la cartella alla fine di ogni percorso nell'elenco visualizzato soddisfi i criteri di ricerca.

## Visualizzazione dei contenuti di una cartella

Selezionare una cartella per visualizzarne i contenuti.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:environment* appropriato.
3. Accedere alla struttura di cartella, espandendo le cartelle necessarie. Oppure immettere criteri di ricerca nel campo apposito per filtrare l'elenco visualizzato in base alle cartelle che iniziano con il nome immesso.
4. Quando viene visualizzata la cartella di destinazione, selezionarla.

   I contenuti di cartella vengono visualizzati in formato tabulare sul riquadro principale.
5. (Facoltativo) Visualizzare i dati nell'ordine desiderato. Fare clic sull'intestazione della colonna su cui si desidera ordinare e selezionare l'ordinamento crescente o decrescente.

## Spostamento di una cartella

È possibile spostare le cartelle in una libreria dell'orchestrator.

**Nota:** per spostare una cartella dalla libreria di un orchestrator a un altro, esportare la cartella (a pagina 363).

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare *Orchestrator:ambiente* con la libreria contenente la cartella sorgente.
3. Accedere alla struttura di cartella, espandendo le cartelle necessarie.

   **Nota:** immettere il nome di cartella parziale per visualizzare le cartelle i cui nomi iniziano con la stringa immessa.

4. Quando viene visualizzata la cartella di destinazione, selezionarla e fare clic su Taglia.
5. Accedere alla cartella di destinazione, quindi fare clic su Incolla.

   Si verifica uno dei seguenti risultati:

   - Se il nome della cartella di destinazione differisce dal nome di quella sorgente, l'orchestrator aggiunge quest'ultima come sottocartella della cartella di destinazione.
   - Se le cartelle sorgente e di destinazione hanno lo stesso nome, l'orchestrator aggiunge i contenuti dell'una nell'altra, unendo così i contenuti delle due cartelle.

## Esportazione di una cartella

Quando si esporta uno degli elementi seguenti, il prodotto crea un file XML che è possibile importare:

- Un oggetto.
- Una cartella che contiene più oggetti necessari nell'orchestrator di destinazione. Gli oggetti possono essere privi di legami tra loro, anche per processi diversi. Il valore Versione di rilascio è non applicabile.
- Una cartella che contiene tutti gli oggetti che compongono una versione di rilascio di un processo. Prima dell'esportazione, definire una versione di rilascio per la cartella e ciascun oggetto nella cartella.

  **Nota:** Per ulteriori informazioni, consultare Scenario: Preparazione di una cartella per l'esportazione come pacchetto di contenuto.

Gli amministratori del contenuto e i responsabili di progettazione dei contenuti possono esportare una cartella dal browser di libreria in un file di esportazione sull'host locale. Il percorso della cartella e la struttura gerarchica degli oggetti e delle cartelle subordinate vengono mantenuti dal file di esportazione.

Gli amministratori possono esportare una cartella in uno dei due modi seguenti:

**Esporta, {Percorsi assoluti | Percorsi relativi}**

L'esportazione modificabile consente ai destinatari nell'ambiente di destinazione di aggiornare nella cartella le versioni degli oggetti esportate.

**Esporta come pacchetto di contenuto {Percorsi assoluti | Percorsi relativi}**

L'esportazione non modificabile non consente ai destinatari nell'ambiente di destinazione di aggiornare le versioni esportate degli oggetti o l'etichetta Versione di rilascio.

**Nota:** Non è possibile esportare gli oggetti che risiedono in più cartelle come collegamenti in un pacchetto. Creare invece una cartella di esportazione e raggruppare tutti gli oggetti da esportare in tale cartella. Per ulteriori informazioni, consultare la *Guida alla progettazione dei contenuti*.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator, quindi selezionare l'elemento *Orchestrator:ambiente* appropriato.
3. Accedere alla cartella da esportare, fare clic con il pulsante destro del mouse sulla cartella e selezionare una delle opzioni seguenti:
   - Esporta, Percorsi assoluti
   - Esporta, Percorsi relativi
4. Per salvare il file .xml, fare clic su Salva nella finestra di dialogo File Download (Download file).

   **Nota:** Il nome predefinito del file è *folder-name*.xml.
5. Sull'unità locale, accedere alla posizione in cui salvare il file XML.
6. Definire il nome desiderato per il salvataggio del file.

   Ad esempio, aggiungere _RP al nome del file per indicare un percorso relativo o _AP per indicare un percorso assoluto.

   `folder-name_RP.xml`

   `folder-name_AP.xml`
7. Fare clic su Salva.

   Il prodotto esporta la cartella e i relativi contenuti.

**Ulteriori informazioni:**

Scenario: Esportazione e importazione degli oggetti in un pacchetto di contenuto (a pagina 372)
Informazioni sulle versioni di rilascio (a pagina 375)

## Importazione di una cartella

Gli amministratori del contenuto possono importare il file XML che rappresenta una cartella esportata e gli oggetti contenuti. Se la cartella è stata esportata con il percorso assoluto, la struttura gerarchica degli oggetti e delle cartelle subordinate viene mantenuta nel file di esportazione. Se la cartella è stata esportata con il percorso relativo, nella cartella di importazione viene creata la struttura dalla cartella di esportazione.

Il processo di importazione è lo stesso a prescindere dalla modalità di esportazione del contenuto. Le opzioni applicabili variano in base al contenuto del file di esportazione.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator*:*ambiente* di destinazione.
3. Accedere alla cartella di destinazione per l'importazione.
4. Fare clic con il pulsante destro del mouse sulla cartella, quindi selezionare Importa.
5. Completare le azioni seguenti nella finestra di dialogo Importazione:
   a. Fare clic su Sfoglia e accedere alla posizione nell'unità locale in cui è stato salvato il file esportato.
   b. Selezionare il file .xml esportato e fare clic su Apri.
   c. Selezionare la modalità di importazione per un oggetto con il nome uguale a quello di un oggetto esistente nello stesso percorso, in base alle informazioni disponibili sugli oggetti presenti nella cartella di importazione.

      **Importa**

      Considerare la versione importata dell'oggetto come una nuova versione dell'oggetto esistente. Selezionare questa opzione se l'importazione è finalizzata all'aggiornamento e si desidera mantenere la cronologia delle versioni precedenti. Se l'oggetto importato ha la stessa versione di rilascio, la versione di rilascio esistente viene sostituita con quella dell'oggetto importato.

      La versione di rilascio dell'oggetto importato prevale se esiste un oggetto analogo con la stessa versione di rilascio.

      **Non importare**

      Interrompere l'importazione dell'oggetto e mantenere l'oggetto esistente. Se si seleziona questa opzione, il processo di importazione elenca gli oggetti con nomi in conflitto. In caso di conflitti, è possibile ripetere l'importazione in una cartella vuota. Altrimenti è possibile rinominare l'oggetto nell'ambiente di origine, quindi ripetere l'esportazione e l'importazione. Questa opzione è consigliata quando gli oggetti in corso di importazione sono nuovi oggetti e non nuove versioni di oggetti esistenti.

      **Importa e sostituisci**

      Eliminare l'oggetto esistente e importare la nuova versione dell'oggetto come versione 0.

   d. Selezionare se impostare la versione degli oggetti nella cartella di importazione come corrente.  La versione corrente del processo è la versione eseguita all'avvio del processo. Questa versione diventa attiva dopo l'importazione. Anche altri processi possono utilizzare gli oggetti usati da questo processo. Se le versioni importate sono già impostate come correnti, è possibile utilizzarle immediatamente. Per ulteriori informazioni, consultare la sezione Definizione dell'importazione di una versione come corrente (a pagina 378).

e. Selezionare se rendere disponibili gli operatori personalizzati.

f. Selezionare se pubblicare il gruppo di operatori personalizzati nella scheda Moduli per il dominio.

   **Nota:** Non pubblicare un gruppo di operatori personalizzati salvo quando la cartella in corso di importazione proviene da un dominio diverso.

6. Fare clic su Invia per avviare il processo di importazione.

7. Fare clic su OK nel messaggio di verifica per la corretta esecuzione dell'importazione.

8. Controllare la cartella importata e i relativi contenuti nella cartella attualmente visualizzata. Si verificano i seguenti risultati:

   - Se la cartella è stata esportata come pacchetto di contenuto:
     - Non è possibile modificare il valore attributo Versione di rilascio per nessun oggetto o per il pacchetto di contenuto.
     - Non è possibile modificare la versione importata di nessun oggetto. Gli oggetti sono di riferimento durante l'importazione.
   - Se è stata selezionata l'opzione per rendere disponibili gli operatori personalizzati durante l'importazione, è possibile utilizzare gli operatori personalizzati importati.
   - Se il gruppo di operatori personalizzati è stato pubblicato nella scheda Moduli, configurare i valori per il gruppo di operatori personalizzati (a pagina 312).

**Ulteriori informazioni:**

Scenario: Esportazione e importazione degli oggetti in un pacchetto di contenuto (a pagina 372)
Informazioni sulle versioni di rilascio (a pagina 375)

## Backup di tutte le cartelle e dei contenuti

È possibile eseguire il backup di una libreria di cartelle e dei relativi contenuti per impedirne la perdita. Richiamare un'esportazione a livello principale della struttura di cartella. Con il processo di esportazione si crea un file .xml con tutte le informazioni necessarie per ricreare le cartelle di libreria e i relativi contenuti dopo l'importazione. Ai fini della protezione si consiglia di archiviare il file .xml in un altro luogo. Se si perde la libreria, è sempre possibile generarla nuovamente importando il file .xml nella directory principale di un nuovo orchestrator.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:ambiente* appropriato.
3. Fare clic con il pulsante destro del mouse sulla cartella principale e selezionare Esporta.
4. Determinare se includere il percorso completo per gli oggetti esportati o il percorso relativo di una cartella contenente l'oggetto.
5. Fare clic su Esporta e selezionare uno dei tipi di percorso seguenti:
   - Percorsi assoluti.
   - Percorsi relativi.

   Su host di Windows, viene visualizzata la finestra di dialogo Download dei file. È possibile selezionare se aprire o salvare il file.
6. Selezionare Salva.

   Su host di Windows, viene visualizzata la finestra di dialogo Salva con nome.
7. Specificare il nome del file con cui salvare il file XML e il percorso. Ad esempio, librarybackup_*date*.xml
8. Fare clic su Salva.

## Eliminazione di una cartella

È possibile eliminare qualsiasi cartella non più necessaria.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:environment* appropriato.
3. Eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse sulla cartella e selezionare Elimina.
   - Selezionare la cartella, quindi fare clic sul pulsante della barra degli strumenti Elimina.

   Viene visualizzato un messaggio di conferma per l'eliminazione.
4. Fare clic su Sì.

   La cartella viene eliminata,

   **Nota:** il cestino contiene sia gli oggetti di automazione eliminati, sia le cartelle eliminate. Quando un oggetto di automazione viene ripristinato, vengono ripristinate anche le cartelle eliminate nel percorso di cartella originale.

# Gestione degli oggetti di automazione

Gli amministratori utilizzano la libreria per gestire gli oggetti di automazione in una struttura di cartella. Le attività di gestione comprendono:

- Impostare un nuovo titolare per oggetti di automazione (a pagina 370).
- Aggiungere tag da utilizzare nelle ricerche di oggetti.
- Gestire le versioni dell'oggetto.
- Eliminare gli oggetti di automazione da una struttura di cartella.
- Spostare un oggetto a un'altra cartella.
- Copiare uno o più oggetti in un orchestrator nello stesso ambiente.

  Consultare le sezioni Esportazione di un oggetto singolo e Importazione di un oggetto singolo.

  Consultare le sezioni Esportazione di una cartella (a pagina 363) e Importazione di una cartella (a pagina 364).

- Copiare gli oggetti in un altro ambiente, ad esempio, da un ambiente di progettazione a uno di produzione.

  Consultare le sezioni Esportazione di una cartella come pacchetto di contenuto (a pagina 376) e Importazione di un pacchetto di contenuto (a pagina 380).

**Ulteriori informazioni:**

Creazione e gestione di cartelle (a pagina 355)

## Impostazione di un nuovo titolare per oggetti di automazione

Solo un amministratore del contenuto o il titolare di un oggetto di automazione può modificare la titolarità di un oggetto di automazione. Per impostazione predefinita, il titolare di un oggetto di automazione è l'ID di accesso dell'utente che crea l'oggetto. Il titolare di un oggetto ha autorizzazioni illimitate su quell'oggetto. Il titolare di un oggetto di automazione o l'amministratore del contenuto può trasferire la titolarità a un altro utente di CA Process Automation. È possibile impostare anche un nuovo titolare per più oggetti che si possiedono.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:environment* appropriato.
3. Selezionare la cartella che contiene gli oggetti di automazione di destinazione.
4. Selezionare uno o più righe sulla griglia per gli oggetti di destinazione.
5. Fare clic su Imposta proprietario.
6. Specificare l'ID utente di CA Process Automation del nuovo titolare.

# Preparazione dell'ambiente di produzione per un nuovo rilascio

I responsabili di progettazione preparano una cartella per l'esportazione come pacchetto di contenuto.

Gli amministratori del contenuto verificano che i touchpoint siano impostati come destinazioni per gli operatori mappati sull'orchestrator o gli agenti nell'ambiente di produzione. Se gli amministratori del contenuto completano la verifica prima dell'importazione, è possibile importare gli oggetti come correnti. Se invece la completano dopo l'importazione, gli oggetti non vengono importati come correnti.

L'utente che esegue l'esportazione e l'importazione verifica che il processo funzioni come progettato nell'ambiente di produzione. Quindi, gli utenti dell'ambiente di produzione possono iniziare a usare il nuovo rilascio.

La transizione comprende le fasi seguenti:

1. Esportare e importare gli oggetti in un pacchetto di contenuto (a pagina 372).
2. Configurare le destinazioni di produzione per il nuovo processo.
3. Verifica del corretto funzionamento del processo come progettato (a pagina 385).
4. Passare il nuovo processo agli utenti dell'ambiente di produzione.

   **Nota:** Il passaggio avviene all'esterno dell'applicazione di CA Process Automation.

## Informazioni sull'esportazione e sull'importazione di un pacchetto di contenuto

Un pacchetto di contenuto viene creato da una cartella che contiene oggetti di automazione relativi a un rilascio specifico. In genere, la cartella contiene gli oggetti seguenti:

- Un processo, il primo rilascio o uno successivo.
- Tutti gli oggetti utilizzati dal processo.
- Tutti gli oggetti necessari per l'esecuzione del processo.

Prima dell'esportazione, aggiungere un valore univoco di versione di rilascio alla cartella e a ciascun oggetto. Inoltre, verificare che ciascun oggetto sia impostato come riferimento. Il riferimento offre una versione statica nell'ambiente di progettazione di ciascun oggetto esistente per questo rilascio.

Quando si esporta una cartella come pacchetto di contenuto, CA Process Automation imposta automaticamente come riferimento tutti gli oggetti nel pacchetto di contenuto al momento dell'importazione. I pacchetti di contenuto e i relativi oggetti non sono modificabili nel nuovo ambiente. Per rendere un oggetto modificabile nell'ambiente di importazione, salvare la versione di riferimento come nuova versione.

### Esempio di versioni di rilascio

La seguente scheda Rilascio per una cartella mostra la proprietà ReleaseVersion. Nell'esempio, il valore è 1.2.3.

L'esempio seguente riguarda la scheda Versioni per un processo, dove il valore Versione di rilascio aggiunto corrisponde a quello aggiunto per la cartella.

La versione di rilascio non è di riferimento. Il pulsante Riferimento è abilitato. Se si nota che un oggetto di destinazione per il rilascio non è di riferimento nell'ambiente di origine, impostare la versione da rilasciare come versione di riferimento.

**Nota:** è possibile esportare contemporaneamente più processi come pacchetto di contenuto in una cartella e utilizzare l'attributo Versione di rilascio per descrivere i contenuti della cartella.

## Scenario: Esportazione e importazione degli oggetti in un pacchetto di contenuto

Utilizzare un pacchetto di contenuto per esportare e importare un set di oggetti correlati che compongono una versione di rilascio da un orchestrator a un altro. Nella maggior parte dei casi, gli orchestrator di origine e di destinazione sono in ambienti differenti. Quando si esporta una cartella come pacchetto di contenuto, il processo di esportazione crea un file .xml sull'unità locale. Quando si esegue l'importazione in un orchestrator diverso, selezionare questo file .xml dall'unità locale. Viene così importato il pacchetto di contenuto.

Esportazione e importazione di oggetti in un pacchetto di contenuto

**Attenersi alla procedura seguente:**

1. Comprendere lo scopo dei pacchetti di contenuto e delle versioni di rilascio. Consultare i seguenti argomenti:
   - Informazioni sui pacchetti di contenuto (a pagina 373)
   - Informazioni sulle versioni di rilascio (a pagina 375)
2. Esportazione di una cartella come pacchetto di contenuto (a pagina 376).
3. Comprendere l'impatto derivato dall'impostazione di diverse opzioni di importazione. Consultare i seguenti argomenti:
   - Definizione dell'importazione di una versione come corrente (a pagina 378)
   - Procedura per impostare le opzioni di importazione (a pagina 378)
4. Importazione di un pacchetto di contenuto (a pagina 380).

**Ulteriori informazioni:**

Esempio: Esportazione e importazione di un pacchetto di contenuto (a pagina 383)

## Informazioni sui pacchetti di contenuto

È possibile esportare gli oggetti nei modi seguenti:

- Un oggetto singolo
- Una cartella
- Una cartella come pacchetto di contenuto

L'esportazione di una cartella come pacchetto di contenuto è diversa dalla semplice esportazione di una cartella nei punti seguenti:

- Il valore della versione di rilascio di qualsiasi oggetto esportato in una *cartella come un pacchetto di contenuto* non può essere modificato dopo l'importazione. (Gli oggetti esportati in una *cartella* non richiedono un valore per la versione di rilascio.)
- Il valore della versione di rilascio di un oggetto esportato in una cartella come un pacchetto di contenuto non può essere modificato dopo l'importazione.

Eseguire l'esportazione di una cartella quando non è necessario assegnare una versione di rilascio ai relativi oggetti. Ad esempio, quando si esportano oggetti da un orchestrator dell'ambiente di progettazione a un altro dello stesso ambiente in una cartella.

Eseguire l'esportazione di una cartella come pacchetto di contenuto quando si esportano oggetti da un ambiente di progettazione a un ambiente di produzione. Generalmente, gli oggetti inclusi in un pacchetto di contenuto rappresentano un rilascio di un processo automatizzato. In questo caso, è necessario mantenere la versione di ciascun oggetto esistente al momento del rilascio. Il pacchetto di contenuto include:

- La versione di rilascio dell'oggetto di processo.
- Tutti gli oggetti utilizzati dal processo.
- Tutti gli oggetti utilizzati dagli utenti dell'ambiente di produzione per avviare il processo o interagire con esso.

Un pacchetto di contenuto è un'unità completa. Un pacchetto di contenuto contiene una cartella di oggetti raggruppati insieme per l'esportazione. Prima dell'esportazione, la versione di ciascun oggetto esportato viene etichettata con un valore Versione di rilascio. Lo stesso valore viene assegnato alla versione di rilascio della cartella.

Il processo di importazione distribuisce tutti gli oggetti del pacchetto di contenuto sulla libreria. Quando viene importato come corrente, l'oggetto è disponibile per l'uso. Gli utenti nell'ambiente di importazione non possono creare né modificare i valori per Versione di rilascio.

Il processo di importazione per un pacchetto di contenuto rende ciascun oggetto di riferimento, con l'obiettivo di utilizzare la versione di rilascio degli oggetti così com'è. Tuttavia, è possibile salvare un oggetto importato come una nuova versione, modificarlo e salvarlo come versione corrente. In un tale caso, la versione di riferimento con il valore Versione di rilascio resta invariata. In questo modo si impedisce un'eventuale modifica pericolosa di tali oggetti. Per annullare eventuali modifiche indesiderate, impostare la versione di riferimento come versione corrente. I responsabili di progettazione dei contenuti addetti alla risoluzione dei problemi sono in grado di identificare le versioni degli oggetti non modificabili che sono stati importati nell'ambiente di produzione.

Se si importa un oggetto da un provider di terze parti in un ambiente di progettazione che si desidera modificare, creare una copia di tale oggetto. Quindi, è possibile aggiornare la copia dell'oggetto e assegnare una versione di rilascio diversa.

## Informazioni sulle versioni di rilascio

Prima di esportare un pacchetto come pacchetto di contenuto che comprende un processo e i relativi oggetti componenti, il responsabile di progettazione dei contenuti compie le azioni seguenti:

- Imposta la versione di rilascio di ciascun oggetto
- Imposta la versione di rilascio della cartella che contiene gli oggetti

Dopo l'importazione, gli oggetti presentano gli stessi valori di versione di rilascio esportati. Quando si esporta una cartella come pacchetto di contenuto, il pacchetto di contenuto importato è in modalità non modificabile. Gli utenti di destinazione non possono modificare il valore Versione di rilascio impostato per questo rilascio. Il valore Versione di rilascio consente ai responsabili di progettazione dei contenuti, che lavorano nell'ambiente di progettazione, di identificare una versione specifica di un oggetto nell'ambiente di produzione.

**Nota:** CA Process Automation imposta il blocco dell'attributo Versione di rilascio sia sull'oggetto, sia sulla versione rilasciata dell'oggetto. Perciò, gli utenti non possono modificare il valore di versione di rilascio per la versione di oggetto importata o quelli impostati per nuove versioni dell'oggetto.

Gli utenti non possono modificare valori di versione di rilascio non modificabile dopo l'importazione. Considerare la necessità delle versioni di rilascio in base alle operazioni da eseguire con gli oggetti. Ad esempio:

- Se si esegue l'esportazione da un ambiente di *progettazione* a un altro, impostare (eventualmente) i valori dell'attributo Versione di rilascio ed esportare la cartella.
- Se si esegue l'esportazione da un ambiente di progettazione a un *ambiente di produzione*, i responsabili di progettazione dei contenuti devono impostare i valori dell'attributo Versione di rilascio per ogni oggetto e per la cartella contenitore. I responsabili di progettazione esportano quindi quella cartella come pacchetto di contenuto.

Le seguenti regole si applicano all'esportazione e all'importazione delle versioni di rilascio:

- Se si verifica una delle condizioni seguenti, le versioni di rilascio sono non modificabili in fase di importazione:
  - Gli oggetti vengono compresi in un pacchetto di contenuto.
  - La versione di rilascio dell'oggetto era non modificabile prima dell'esportazione.
- CA Process Automation imposta come riferimento le versioni importate quando gli oggetti vengono importati come pacchetto di contenuto, con versioni di rilascio non modificabili.

  **Nota**: Se un oggetto viene importato nuovamente con la stessa versione di rilascio, quell'oggetto viene sovrascritto.

Le seguenti regole si applicano per copiare e incollare gli oggetti importati:

- La prima versione della copia di oggetto mantiene il valore Versione di rilascio, se è modificabile.
- Se la versione corrente dell'oggetto originale è di riferimento e l'attributo Versione di rilascio dell'oggetto è non modificabile, anche la copia è di riferimento.

## Esportazione di una cartella come pacchetto di contenuto

I responsabili di progettazione dei contenuti preparano gli oggetti associati alla stessa versione di rilascio per l'esportazione. In seguito, il pacchetto di contenuto viene esportato da un responsabile di progettazione dei contenuti o da un amministratore. La procedura seguente riguarda entrambe le fasi di preparazione ed esportazione.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator*:*ambiente* di origine.
3. Accedere alla cartella di destinazione. Verificare che la cartella contenga tutti gli oggetti che si desiderano esportare. Verificare che la cartella contenga solo gli oggetti che si desiderano esportare.
4. Aggiungere la versione di rilascio alla cartella di destinazione:
    a. Nel riquadro di navigazione, selezionare la cartella che contiene la cartella da esportare.
    b. Nel riquadro principale, fare clic con il pulsante destro del mouse sulla cartella da esportare e selezionare Proprietà.
    c. Fare clic sulla scheda Rilascio.
    d. Fare doppio clic sulla colonna Valore nella riga ReleaseVersion.
    e. Immettere la versione di rilascio nella finestra di dialogo Valore e fare clic su OK.
    f. Fare clic su Salva.

5. Aggiungere la versione di rilascio alla versione selezionata di ciascun oggetto nella cartella di destinazione e verificare che la versione selezionata sia Con riferimento.

   a. Selezionare la cartella di destinazione che contiene gli oggetti da esportare.

   b. Fare clic con il pulsante destro del mouse su un oggetto e selezionare Proprietà.

   c. Fare clic sulla scheda Rilascio.

   d. Fare clic con il pulsante destro del mouse sulla riga della versione da esportare, selezionare Imposta versione di rilascio e immettere lo stesso valore di versione di rilascio assegnato alla cartella, quindi fare clic su OK.

   e. Se il valore Riferimento per la riga selezionata è No, fare clic sulla scheda Versioni, quindi su Riferimento. Fare clic su Sì per confermare il riferimento.

      **Nota:** È importante impostare gli oggetti di riferimento prima dell'esportazione, in modo da avere sempre un'immagine salvata nell'ambiente di progettazione di ciascun oggetto al momento del rilascio. Tutti gli oggetti sono impostati automaticamente come riferimento durante il processo di importazione.

   f. Fare clic su OK.

   g. Ripetere queste fasi per ciascun oggetto nella cartella.

6. Nel riquadro di navigazione, fare clic con il pulsante destro del mouse sulla cartella, quindi selezionare una delle opzioni seguenti:

   - Esporta come pacchetto di contenuto, Percorsi assoluti

     Include il percorso completo della cartella selezionata.

   - Esporta come pacchetto di contenuto, Percorsi relativi

     Include il percorso relativo alla cartella contenente quella selezionata.

7. Salvare il file del pacchetto esportato.

   a. Fare clic su Salva per salvare il file .xml.

   b. Accedere a una cartella sull'unità locale e fare clic su Salva.

   c. Quando viene visualizzata la finestra di dialogo di download completato, fare clic su Chiudi.

   CA Process Automation esporta il pacchetto di contenuto come file .xml. Il pacchetto di contenuto è pronto per l'importazione in un altro orchestrator. Il file *folder-name*.xml viene crittografato.

## Definizione dell'importazione di una versione come corrente

Durante un'importazione, viene specificato se importare gli oggetti come correnti. Importare oggetti come correnti quando si verificano entrambe le condizioni seguenti:

- Tutte le destinazioni sono definite come touchpoint, touchpoint proxy o gruppo touchpoint.
- Le destinazioni di produzione per il nuovo processo sono configurate.

**Nota:** è possibile importare un processo come corrente quando le destinazioni sono espressioni che puntano alle variabili in un set di dati. Durante l'importazione è possibile modificare le variabili nel set di dati per fare riferimento ai touchpoint di produzione.

CA Process Automation richiede di attendere dopo l'importazione per eseguire il mapping delle destinazioni di operatore sugli host di produzione solo se una destinazione è definita come ID agente, indirizzo IP o nome host. In questo caso, non importare gli oggetti come correnti. Aggiornare invece le destinazioni negli operatori dopo l'importazione, quindi contrassegnare la versione importata come corrente.

## Procedura per impostare le opzioni di importazione

CA Process Automation offre una certa flessibilità nell'importazione degli oggetti.

Se l'importazione comprende operatori personalizzati, selezionare Rendi disponibili gli operatori personalizzati importati.

Se gli operatori personalizzati sono nuovi e appartengono a un nuovo gruppo personalizzato, esguire l'azione adeguata per l'ambiente in uso.

- Non selezionare Pubblica configurazione del gruppo di operatori personalizzati se l'ambiente di importazione si trova nello stesso dominio dell'ambiente di esportazione. In questo caso, la configurazione del gruppo di operatori personalizzati è già pubblicata.
- Selezionare Pubblica configurazione del gruppo di operatori personalizzati se l'ambiente di importazione si trova in un dominio diverso dall'ambiente di esportazione

Tenere conto del contenuto importato quando si configura l'opzione Imposta la versione importata come corrente e si seleziona la modalità di gestione dei nomi duplicati.

- Per attivare gli oggetti importati, con la possibilità di ripristinare la versione precedente di un oggetto importato, se necessario:
  - Selezionare Importa
  - Selezionare Imposta la versione importata come corrente

  **Nota:** Queste opzioni sono indicate quando è in corso l'importazione di una versione di rilascio di aggiornamento e tutte le destinazioni dell'operatore sono impostate su host nell'ambiente di importazione. È possibile ricevere una notifica sui nomi duplicati perché gli oggetti dell'ultima release si trovano nella cartella di destinazione.

- Per eseguire l'importazione senza attivare gli oggetti aggiornati, in cui la versione precedente conserva lo stato di versione corrente:
  - Selezionare Importa
  - Deselezionare Imposta la versione importata come corrente

  **Nota:** Queste opzioni sono indicate quando l'importazione include operatori che utilizzano come destinazione host non ancora definiti con il relativo nome touchpoint nell'ambiente di importazione. Con questa impostazione è possibile rendere correnti gli oggetti dopo aver accertato che le destinazioni del processo sono disponibili nell'ambiente di importazione.

- Per rinviare l'importazione di qualsiasi oggetto con un nome duplicato e rendere correnti gli oggetti in modo manuale:
  - Selezionare Non importare
  - Deselezionare Imposta la versione importata come corrente
  - **Nota:** Queste opzioni sono indicate quando è in corso l'importazione di oggetti nuovi in una cartella popolata. Queste opzioni evitano di rendere un oggetto importato una nuova versione di un oggetto con lo stesso nome ma con una funzione diversa. Queste opzioni consentono inoltre di rendere correnti gli oggetti dopo la fase di test e verifica del loro utilizzo nel nuovo ambiente.

    Se si ricevono avvisi, considerare le azioni seguenti:

    - Registrare i nomi duplicati nel messaggio di avviso e informare un amministratore nell'ambiente di origine. Forse è possibile rinominare tali oggetti ed esportarli di nuovo.
    - Eseguire una nuova importazione, ma in una cartella vuota.

- Per attivare gli oggetti importati senza la possibilità di annullare l'azione per gli oggetti con nomi duplicati:
  - Selezionare Importa e sostituisci
  - Selezionare Imposta la versione importata come corrente
  - **Nota:** Queste opzioni sono indicate quando si importano nuove correzioni agli oggetti nella cartella di destinazione. In questo caso, non è necessario ripristinare la versione sostituita.

## Importazione di un pacchetto di contenuto

Gli amministratori selezionano l'orchestrator, selezionano la cartella di destinazione e, quindi, richiamano l'importazione. Se con l'importazione viene creato un pacchetto di contenuto, questo contiene un insieme di oggetti di riferimento per lo stesso rilascio. Non è possibile modificare i valori della versione di rilascio degli oggetti in un pacchetto di contenuto importato.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:ambiente* di destinazione.

3. Fare clic con il pulsante destro del mouse sulla cartella di destinazione e selezionare Importa.
4. Fare clic su Sfoglia e accedere alla posizione nell'unità locale in cui è stato salvato il file esportato. Selezionare il file .xml esportato e fare clic su Apri.
5. Selezionare la procedura di importazione dell'oggetto con il nome uguale a quello di un oggetto esistente nello stesso percorso.
   - Selezionare Importa per importare ciascun oggetto come nuova versione dell'oggetto esistente.

     Questa opzione è indicata per un aggiornamento quando si desidera conservare la cronologia delle versioni precedenti.

     **Nota:** Se un oggetto esistente ha la stessa versione di rilascio dell'oggetto importato, l'oggetto importato sostituisce la versione duplicata.
   - Selezionare Non importare per interrompere l'importazione dell'oggetto e mantenere l'oggetto esistente.

     Se si seleziona questa opzione, il processo di importazione elenca gli oggetti con nomi in conflitto. In caso di conflitti, è possibile ripetere l'importazione in una cartella vuota. Altrimenti è possibile rinominare l'oggetto nell'ambiente di origine, quindi ripetere l'esportazione e l'importazione. Questa opzione è consigliata quando gli oggetti in corso di importazione sono nuovi oggetti e non nuove versioni di oggetti esistenti.
   - Selezionare Importa e sostituisci per eliminare l'oggetto esistente e importare la nuova versione dell'oggetto come versione 0.
6. Selezionare se impostare la versione degli oggetti nella cartella di importazione come corrente.
   - Selezionare Imposta la versione importata come corrente per attivare la versione importata immediatamente dopo l'importazione. Se l'oggetto importato è un aggiornamento, i processi esistenti che utilizzavano la versione precedente degli oggetti ora utilizzano la versione importata. Gli oggetti importati possono includere un processo con le destinazioni dell'operatore configurate nell'ambiente di importazione. In questo caso, è possibile verificare il processo aggiornato senza reimpostare le versioni.
   - Deselezionare l'opzione Imposta la versione importata come corrente per rinviare l'impostazione della versione corrente per un processo manuale. Ad esempio, deselezionare questa opzione se l'importazione contiene un processo in cui le destinazioni degli operatori non sono state ancora definite in questo ambiente.

7. Selezionare se rendere disponibili gli operatori personalizzati importati.
   - Selezionare Rendi disponibili gli operatori personalizzati importati per impostare in modo automatico tutti gli operatori personalizzati importati come disponibili.
   - Deselezionare Rendi disponibili gli operatori personalizzati importati per mantenere gli operatori personalizzati importati in stato non disponibile e renderli disponibili manualmente uno per uno.
8. Selezionare se pubblicare un gruppo di operatori personalizzati nella scheda Moduli.
   - Selezionare Pubblica configurazione del gruppo di operatori personalizzati se l'importazione include nuovi operatori personalizzati e un nuovo gruppo di operatori personalizzati e avviene verso un dominio diverso da quello di esportazione.
   - Deselezionare Pubblica configurazione del gruppo di operatori personalizzati nei casi seguenti:
     - L'ambiente di importazione si trova nello stesso dominio dell'ambiente di esportazione.
     - Gli operatori personalizzati importati sono nuovi rilasci di operatori personalizzati esistenti. In questo caso, esistono gruppi di operatori personalizzati.
     - Si preferisce che sia un amministratore a pubblicare manualmente la configurazione di un nuovo gruppo di operatori personalizzati.
9. Fare clic su Invia per avviare il processo di importazione.
10. Fare clic su OK nel messaggio di verifica per la corretta esecuzione dell'importazione.

    Il pacchetto viene importato correttamente nella cartella selezionata. Inoltre, il pacchetto viene visualizzato nel riquadro Pacchetti di contenuto della scheda Operazioni. Quando si seleziona un pacchetto di contenuto dal riquadro, vengono visualizzate le proprietà. La proprietà visualizzata è il valore ReleaseVersion impostato per la cartella prima dell'esportazione come pacchetto di contenuto.

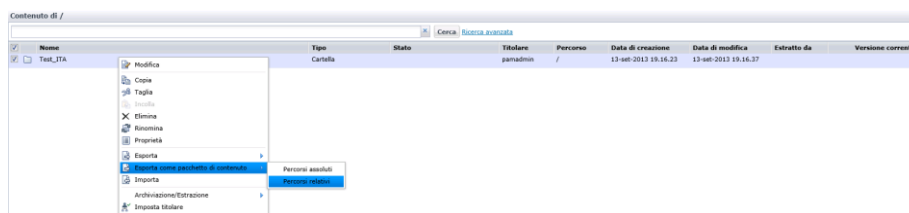
## Esempio: Esportazione e importazione di un pacchetto di contenuto

Esportare una cartella come pacchetto di contenuto dalla libreria dell'ambiente di origine (progettazione) e salvare il file .xml risultante. Importare un pacchetto nella libreria dell'ambiente di destinazione (produzione) selezionando il file .xml e specificando le opzioni di importazione.

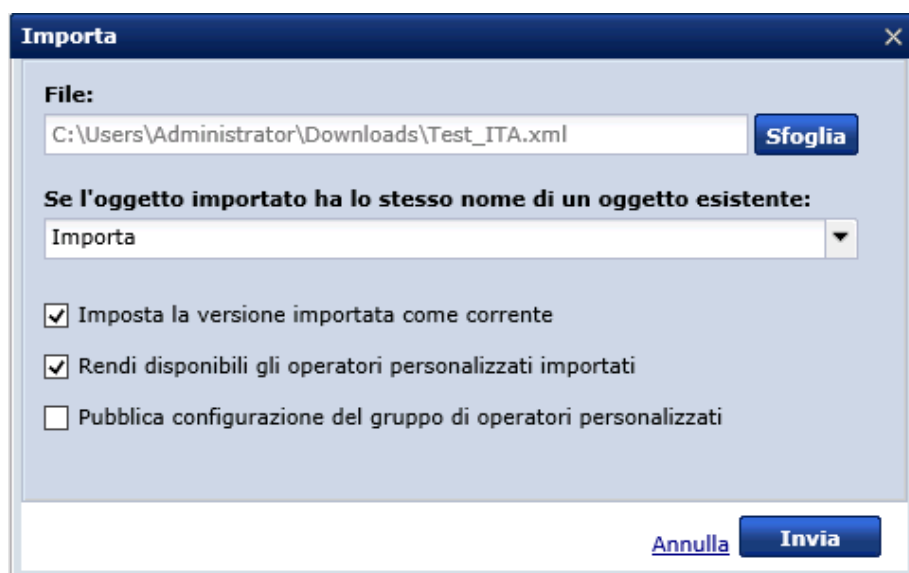
### Esportazione come pacchetto di contenuto

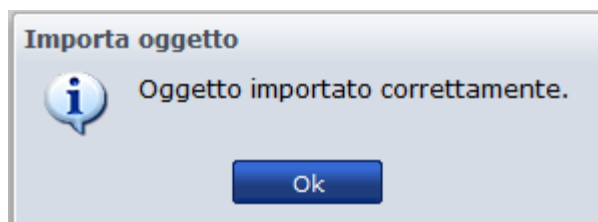
1. Fare clic sulla scheda Libreria per l'elemento *Orchestrator*:*ambiente* contenente la cartella con l'oggetto di cui eseguire la transizione.
2. Fare clic con il pulsante destro del mouse sulla cartella, quindi selezionare Esporta come pacchetto di contenuto, Percorsi relativi.

   Questa selezione copia il pacchetto in una cartella diversa dalla principale.

*Equation 1: Il menu di scelta rapida per una cartella comprende le opzioni Esporta ed Esporta come pacchetto di contenuto.  Entrambe le opzioni di esportazione consentono di selezionare Percorsi assoluti e Percorsi relativi.*

3. Salvare il file in una cartella sull'unità locale o su un'unità mappata.
4. Fare clic su Open Folder (Apri cartella). Viene visualizzata la cartella in cui è stato salvato il file XML dell'esportazione una volta completato il download.

### Importazione di un pacchetto di contenuto

1. Fare clic sulla scheda Libreria e selezionare l'elemento *Orchestrator*:*ambiente* che è la destinazione del processo di esportazione e importazione.
2. Accedere alla cartella in cui importare il file .xml, fare clic con il pulsante destro del mouse sul file e selezionare Importa.

3. Fare clic su Sfoglia, accedere alla posizione in cui è stato esportato il file, quindi fare clic su Apri.

   In questo esempio, selezionare le opzioni seguenti:

   - Importa
   - Imposta la versione importata come corrente
   - Rendi disponibili gli operatori personalizzati importati

     **Nota:** se non si seleziona questa opzione, CA Process Automation importa gli operatori personalizzati come non disponibili.

     **Nota:** Non selezionare Pubblica configurazione del gruppo di operatori personalizzati quando il pacchetto di importazione contiene uno o più operatori personalizzati per cui è stato pubblicato un nuovo gruppo di operatori personalizzati nel dominio di appartenenza dell'ambiente di importazione. Il gruppo pubblicato già esiste nella scheda Moduli del browser di configurazione in caso di esportazione e importazione tra ambienti nello stesso dominio.

4. Fare clic su Invia.
5. Fare clic su OK nel messaggio di conferma.

Il pacchetto di contenuto importato viene visualizzato nella cartella di importazione selezionata. È possibile trovare i pacchetti di contenuto anche nel riquadro Pacchetti di contenuto della scheda Operazioni. Se si fa clic sul pacchetto di contenuto nel riquadro a sinistra, le relative proprietà vengono visualizzate nel riquadro a destra.

6. Dalla cartella di importazione, selezionare il pacchetto di contenuto importato e fare clic su Proprietà.
7. Fare clic sulla scheda Rilascio.

   I dati per la versione di rilascio del pacchetto di contenuto sono uguali a quelli in fase di esportazione. Passando il puntatore del mouse sul campo Versione di rilascio, la descrizione comando indica che non è possibile modificare il valore Versione di rilascio.
8. Fare doppio clic sul pacchetto di contenuto e notare quanto segue:
   - Tutti gli oggetti importati sono visualizzati nella stessa cartella di destinazione.
   - Tutti gli oggetti importati sono di riferimento.
   - Tutti gli oggetti importati hanno lo stesso testo per la versione di rilascio impostata per l'oggetto prima dell'esportazione.

## Verifica del corretto funzionamento del processo come progettato

Prima di trasferire i contenuti di un pacchetto di contenuto importato per l'uso di produzione, l'amministratore esegue il processo e controlla i risultati. Un'esecuzione corretta implica che l'importazione del pacchetto di contenuto comprenda tutti i componenti degli oggetti richiesti e che tutte le destinazioni siano configurate correttamente.

La fase di verifica può includere il controllo del corretto funzionamento per il meccanismo di avvio automatizzato, se si tratta di pianificazione, moduli o trigger. Attivare i trigger, se necessario.

Nel modulo più semplice, è possibile riassumere il processo di verifica come segue.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria e selezionare **Orchestrator**:*ambiente* per la destinazione dell'importazione.
2. Fare clic sulla scheda Operazioni.
3. Avviare il processo mediante il meccanismo di avvio pianificato.
4. Controllare il processo in esecuzione fino al completamento. Rispondere a qualsiasi modulo affinché il processo possa continuare.

5. Se il processo non è eseguito correttamente, restituirlo al responsabile di progettazione dei contenuti per risolvere i problemi.
6. Se il processo contiene rami, creare i casi per la verifica dei rami. Quindi, avviare il processo e monitorarlo.
7. Eseguire una delle seguenti azioni:
   - Se il processo non è eseguito correttamente, restituirlo al responsabile di progettazione dei contenuti per risolvere i problemi.
   - Se il processo viene eseguito correttamente, passarlo all'amministratore di produzione.
8. Se si identifica un oggetto che necessita di ulteriore progettazione, procedere come segue:
   a. Un responsabile di progettazione dei contenuti risolve il problema e testa l'oggetto per verificarne il corretto funzionamento.
   b. I responsabili di progettazione preparano una nuova cartella per l'esportazione come pacchetto di contenuto. Questo implica l'impostazione di una nuova versione di rilascio per la cartella e per tutti gli oggetti compresi nel rilascio. Consultare la sezione Scenario: Preparazione di una cartella per l'esportazione come pacchetto di contenuto.
   c. Eseguire nuovamente l'esportazione e l'importazione della cartella come pacchetto di contenuto. Consultare la sezione Scenario: Esportazione e importazione degli oggetti in un pacchetto di contenuto (a pagina 372).
   d. Verificare nuovamente il corretto funzionamento del processo automatizzato come progettato.

**Ulteriori informazioni:**

Preparazione dell'ambiente di produzione per un nuovo rilascio (a pagina 370)

# Utilizzo del cestino

Il cestino contiene cartelle e oggetti eliminati dalla libreria da qualsiasi utente.

L'azione di *eliminazione definitiva* consente di eliminare in modo permanente gli oggetti o le cartelle selezionati dalla libreria.

L'azione di *ripristino* consente di ripristinare gli oggetti o le cartelle selezionati. Il ripristino include qualsiasi cartella eliminata in precedenza nel percorso degli oggetti ripristinati.

Per informazioni, selezionare l'azione che si desidera eseguire:

- Ricerca nel cestino (a pagina 388)
- Ripristino di oggetti e cartelle (a pagina 389)
- Eliminazione definitiva di oggetti e cartelle (a pagina 390)

## Ricerca nel cestino

È possibile eseguire una query nel cestino con una ricerca di base o una ricerca avanzata. La ricerca di base applica il filtro sul nome quando la voce corrisponde al nome intero o a una stringa con l'inizio uguale a determinati nomi. La ricerca avanzata offre molti criteri di ricerca.

**Attenersi alla procedura seguente:**

1. Aprire la scheda Libreria, comprimere la cartella principale e selezionare Cestino.

   Nel riquadro principale sono visualizzati tutti gli oggetti di automazione e le cartelle attualmente eliminati.

2. Immettere una stringa con un asterisco (*) nel campo di ricerca e fare clic su Cerca per eseguire una ricerca di base. Ad esempio, immettere Custom* per limitare la visualizzazione a oggetti che iniziano con la stringa Custom.

   Le cartelle e gli oggetti di automazione con nomi che corrispondono alla voce immessa vengono visualizzati nell'elenco filtrato.

3. Fare clic sulla Ricerca avanzata per visualizzare gli attributi da cercare. È possibile immettere uno o più tipi di criteri di ricerca.

   - Parole chiave: immettere una o più parole chiave per trovare oggetti o cartelle assegnati alle parole chiave specificate. Se si specificano più parole chiave, utilizzare la virgola (,) come delimitatore.
     - Per filtrare in base agli oggetti definiti con una qualsiasi parola chiave specificata, selezionare OPPURE, il valore predefinito.
     - Per filtrare in base agli oggetti definiti con tutte le parole chiave specificate, selezionare E.
   - Nome: nome della cartella o dell'oggetto di automazione.
   - Titolare: l'ID utente del titolare dell'oggetto o della cartella. Il titolare predefinito è l'utente che ha creato l'oggetto. È possibile specificare un nuovo titolare con l'opzione Imposta titolare.
   - Tipo: selezionare un tipo di oggetto di automazione dall'elenco a discesa.
   - Stato: selezionare uno stato dall'elenco a discesa.
   - Data di modifica: utilizzare i calendari per selezionare l'intervallo di date in cui sono stati modificati gli elementi da visualizzare.
   - Data di creazione: utilizzare i calendari per selezionare l'intervallo di date in cui sono stati creati gli elementi da visualizzare.

4. Fare clic su Cerca.

5. Applicare l'azione di eliminazione definitiva o ripristino sul set di risultati.

6. Fare clic su Reimposta per cancellare i criteri di ricerca se si desidera passare subito a un'altra ricerca.

## Ripristino di oggetti e cartelle

Gli oggetti o le cartelle eliminati dalla libreria vengono spostati nel cestino. Dal cestino è possibile ripristinare una cartella o un oggetto eliminato. Il processo di ripristino consente di ripristinare l'oggetto o la cartella e ulteriori cartelle nel percorso eliminato. È possibile specificare se sovrascrivere gli oggetti nel percorso di destinazione che hanno lo stesso nome degli oggetti selezionati.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria, contrarre la cartella principale nel riquadro sinistro e selezionare Cestino.

   La griglia principale viene aggiornata per mostrare tutti gli oggetti di automazione e le cartelle attualmente presenti nel cestino.

2. Selezionare uno o più oggetti o cartelle, quindi fare clic su Ripristina selezione.

3. Fare clic su Sì nel messaggio di conferma per il ripristino.

   - Se il percorso di destinazione non contiene oggetti con lo stesso nome dell'oggetto selezionato, quest'ultimo viene ripristinato nella posizione di destinazione.
   - Se un oggetto nel percorso di destinazione presenta lo stesso nome dell'oggetto selezionato per il ripristino, viene visualizzato un avviso. Eseguire una delle seguenti azioni:
     - Selezionare l'oggetto e fare clic su OK per continuare il processo di ripristino.

       L'oggetto viene spostato dal cestino al percorso di destinazione, sostituendo l'oggetto presente nel percorso di destinazione.
     - Fare clic su Annulla per arrestare il processo di ripristino per l'oggetto.

       L'oggetto non viene sostituito nel percorso di destinazione. In questo caso, valutare se spostare o rinominare l'oggetto con il nome duplicato, quindi ripetere il processo di ripristino.

   Il processo di ripristino consente di ripristinare gli oggetti selezionati e, se necessario, i relativi percorsi di cartella.

## Eliminazione definitiva di oggetti e cartelle

Il cestino è inteso come un contenitore temporaneo per gli oggetti eliminati, in modo che i responsabili di progettazione dei contenuti possano ripristinare gli oggetti eliminati involontariamente.

Eliminando regolarmente gli oggetti obsoleti in modo definitivo, si ottiene un cestino ordinato. In qualità di amministratore, è possibile eliminare in modo definitivo le cartelle e gli oggetti di automazione selezionati. In alternativa, è possibile eliminare in modo definitivo i contenuti del cestino in una sola fase. Non è possibile recuperare o ripristinare un oggetto eliminato in modo definitivo.

**Attenersi alla procedura seguente:**

1. Fare clic sulla scheda Libreria.
2. Fare clic su Orchestrator e selezionare l'elemento *Orchestrator:ambiente* appropriato.
3. Se il cestino non è visibile, comprimere la cartella principale.
4. Fare clic su Cestino.

   Nella griglia del riquadro generale vengono visualizzati tutti gli oggetti di automazione e le cartelle eliminati dalla libreria.
5. Eseguire una delle seguenti azioni:
   - Selezionare oggetti specifici, quindi fare clic su Elimina selezione.
   - Fare clic su Elimina tutto.
6. Quando si avvia l'eliminazione definitiva per gli oggetti selezionati, viene visualizzato un messaggio di conferma.
   - Fare clic su No per annullare l'eliminazione definitiva, ripristinare gli oggetti richiesti nella Libreria, riavviare l'eliminazione definitiva.
   - Fare clic Sì per proseguire con il processo di eliminazione definitiva.
7. Quando si avvia un'eliminazione definitiva di tutti i processi in cui i contenuti del cestino includono degli oggetti estratti, viene visualizzata una finestra di dialogo che elenca tali oggetti. Valutare l'elenco ed eseguire una delle azioni seguenti:
   - Fare clic su No per annullare l'eliminazione definitiva, ripristinare gli oggetti richiesti nella Libreria, riavviare l'eliminazione definitiva.
   - Fare clic Sì per proseguire con il processo di eliminazione definitiva.

# Appendice A: Supporto per FIPS 140-2

La pubblicazione Federal Information Processing Standard (FIPS) 140-2, *Requisiti di sicurezza per i moduli crittografici,* definisce un insieme di requisiti per i prodotti che crittografano i dati sensibili. Lo standard fornisce quattro livelli di protezione finalizzati a coprire un ampio intervallo di applicazioni e ambienti potenziali. Il reparto Security Management and Assurance (SMA) di NIST convalida i moduli di crittografia e le implementazioni degli algoritmi crittografici. Una volta eseguita la convalida, SMA pubblica il vendor e i numeri dei certificati di convalida con i nomi dei moduli.

Per supportare FIPS 140-2, CA Process Automation utilizza i moduli crittografici convalidati dalle librerie Crypto-J di RSA BSAFE®. RSA è una divisione EMC per la sicurezza.

Questa sezione contiene i seguenti argomenti:



## Casi di utilizzo della crittografia in CA Process Automation

CA Process Automation esegue la crittografia della comunicazione e degli archivi di dati. CA Process Automation utilizza moduli conformi allo standard FIPS 140-2 come necessario ai fini della protezione.

Ad esempio:

- Durante il trasferimento di dati tra l'orchestrator e gli agenti, i dati vengono crittografati.
- Durante il trasferimento di dati dall'orchestrator al client CA Process Automation, i dati sensibili vengono crittografati.
- Durante il trasferimento di dati tra CA EEM e CA Process Automation, i dati vengono crittografati. (Versione 03.1.00 e successive).
- Durante il trasferimento di un sistema composto da oggetti di automazione mediante esportazione e importazione, tutti gli oggetti Password nel sistema vengono crittografati.
- Quando qualsiasi dato sensibile, come le password, è archiviato nei file system, quei dati vengono crittografati.

# Modulo di crittografia con convalida FIPS 140-2

CA Process Automation utilizza un modulo di crittografia integrato, con convalida FIPS 140-2 e le specifiche seguenti:

- Cert. n. 1048
- Vendor: RSA, Divisione EMC per la sicurezza
- Modulo di crittografia: RSA BSAFE® Crypto-J JCE Provider Module (Versione software: 4.0)
- Tipo di modulo: Software
- Date di convalida: 27/10/2008; 26/01/2009; 07/09/2010
- Livello/descrizione: Livello complessivo 1
- Algoritmo approvato da FIPS: RSA (Cert. #311)

Per maggiorni informazioni, eseguire una ricerca su Internet per *trovare la policy sulla sicurezza per il modulo del provider JCE di Crypto-J di RSA BSAFE*. Questa policy elenca le piattaforme a cui gli algoritmi sono conformi, incluse piattaforme Microsoft, Linux, Oracle (Solaris), HP e IBM. Inoltre, include informazioni dettagliate sugli algoritmi Crypto-J conformi a FIPS.

In modalità solo FIPS, CA EEM utilizza gli algoritmi seguenti:

- SHA1, SHA256, SHA384: per gestire la comunicazione client-server.
- SHA512: per archiviare le password utente.

  **Nota**: CA EEM applica SHA512 al digest password solo se si aggiorna il digest password. Finché non si esegue l'aggiornamento, CA EEM accetta la password esistente nel digest password.

- SHA256: per gestire i certificati dell'applicazione.
- TLS v1.0: per la comunicazione con directory LDAP esterne se la connessione LDAP avviene su TLS.

# Gestione degli indirizzi IP

Potrebbe risultare necessario gestire gli indirizzi IP e/o i nomi. Seguono gli esempi:

- Modificare l'indirizzo IP e il nome di un orchestrator.

  Modificare la combinazione di nome e indirizzo IP ogni volta che compaiono nei file seguenti.

  `install_dir/server/c2o/.config/OasisConfig.properties`

  `install_dir/server/c2o/.config/Domain.xml`

  **Nota:** per continuare a utilizzare un nome host invariato in tutti i riferimenti in CA Process Automation, modificare il DNS con il nuovo indirizzo IP.

- Se si installano gli agenti mediante indirizzi IP che cambiano, riconfigurare l'agente aggiornando il file seguente:

  `install_dir/PAM Agent/PAMAgent/.config/OasisConfig.properties`

  Modificare il valore della proprietà seguente:

  `oasis.jxta.host`

- Utilizzare più indirizzi IP per CA Process Automation se si dispone di due NIC, una interna e una esterna.

  Per associare CA Process Automation all'indirizzo IP esterno, aggiungere la proprietà seguente a OasisConfig.properties:

  `jboss.bind.address=xxx.xxx.xxx.xxx`

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

# Autenticazione e autorizzazione utente in modalità FIPS

È possibile configurare CA EEM per l'utilizzo della modalità FIPS. Questa opzione è facoltativa. Solo se CA EEM è configurato per l'utilizzo della modalità FIPS, è possibile configurare CA Process Automation allo stesso modo. Anche se CA EEM è configurato per l'utilizzo della modalità FIPS, è possibile configurare CA Process Automation per non utilizzarla.

A seconda se modalità FIPS è attivata o disattivata, i dati trasferiti tra CA EEM e CA Process Automation vengono crittografati. La differenza consiste negli algoritmi utilizzati per la crittografia.

Quando gli utenti accedono, CA Process Automation trasferisce il nome utente e la password a CA EEM. CA EEM restituisce i dati di autenticazione e autorizzazione a CA Process Automation.

- Quando la modalità FIPS è attiva:
  - I dati trasferiti vengono crittografati con l'algoritmo SHA1 supportato da FIPS.
  - Viene utilizzato un certificato PAM.cer.
- Quando la modalità FIPS è disattivata:
  - I dati trasferiti vengono crittografati con l'algoritmo MD5.
  - Viene utilizzato un certificato PAM.p12.

# Appendice B: Gestione del dominio

La gestione del dominio include alcune attività che vengono eseguite all'esterno della scheda Configurazione.

Questa sezione contiene i seguenti argomenti:



## Creazione del dominio

La creazione di un sistema comprende modifiche sia fisiche, sia logiche. Il proprio sistema viene creato fisicamente con l'installazione e logicamente in CA Process Automation.

- Se occorre maggiore capacità nell'ambiente di progettazione, aggiungere un nodo all'orchestrator di dominio.
- Se occorre maggiore capacità nell'ambiente di produzione, aggiungere un nodo all'orchestrator utilizzato per la produzione. Aggiungere un bilanciatore del carico hardware o software.

  **Nota:** per informazioni, consultare la *Guida all'installazione.*

- Se un server su cui è installato un orchestrator è in disservizio, esportare il nodo principale della libreria e importarlo in un nuovo orchestrator.
- Quando sono richiesti nuovi utenti o vengono aggiunti nuovi ruoli, aggiornare CA EEM con le modifiche apportate agli account utente e alle norme.

# Backup del dominio

Eseguire il backup di CA Process Automation mediante lo strumento apposito utilizzato presso la propria organizzazione.

**Attenersi alla procedura seguente:**

1. Eseguire il backup di ciascuna occorrenza dei tre database di CA Process Automation seguenti:
   - Repository
   - Runtime
   - Reporting
2. Eseguire il backup della seguente directory:

   *install_dir*/server/c2o/.config
3. Eseguire il backup dei contenuti della libreria esportando la cartella principale nella scheda Libreria.

# Ripristino del dominio dal backup

L'esecuzione di CA Process Automation può non riuscire a causa di dati danneggiati, configurazione errata o perdita di dati archiviati su un orchestrator di dominio cluster. È possibile risolvere l'errore e ripristinare i dati in CA Process Automation.

È possibile ripristinare CA Process Automation dopo un errore. È necessario eseguire una nuova installazione dell'orchestrator di dominio, da arrestare appena installato. Sostituire i database vuoti con i backup di database e ripristinare il file di configurazione da un backup. Quindi, avviare CA Process Automation e verificare che i dati ripristinati siano presenti.

**Attenersi alla procedura seguente:**

1. Preparare l'installazione. Consultare la *Guida all'installazione* appena completata la preparazione seguente:
   - Verificare che l'hardware, il sistema operativo e il motore di database siano installati.
   - Verificare che i componenti di terze parti richiesti siano installati.
   - Installare e configurare CA EEM.
2. Eseguire una nuova installazione di CA Process Automation come descritto nella *Guida all'installazione*.
3. Aggiungere i nodi necessari per riflettere il cluster originale. Per informazioni, consultare la *Guida all'installazione*.
4. Interrompere CA Process Automation.
5. Ripristinare il sistema dal backup.
   a. Sostituire il repository database, il database di runtime e il database di reporting con i rispettivi backup.
   b. Rinominare la cartella corrente .config:

      *install_dir*/server/c2o/.config
   c. Ripristinare quanto segue dal backup:

      *install_dir*/server/c2o/.config
6. Avviare CA Process Automation.
7. Verificare che la configurazione sia stata ripristinata.
8. Verificare che i dati di database siano intatti.

# Gestione certificati

Le gestione dei certificati include le procedure seguenti:

- Installazione del certificato predefinito CA Process Automation. (a pagina 399)
- Creazione e implementazione dei propri certificati per CA Process Automation. (a pagina 401)
- Implementazione del proprio certificato SSL attendibile di terze parti per CA Process Automation. (a pagina 404)

## Modalità di protezione delle password in CA Process Automation

Le credenziali dell'account utente, il nome utente e la password sono utilizzati per accedere a vari sistemi e funzionalità. La password deve essere protetta per motivi di sicurezza. Sebbene le password siano stringhe, vengono considerate diversamente da altri valori di questo tipo di dati. CA Process Automation protegge le password a livello di interfaccia utente nei seguenti modi:

- Gli utenti non possono passare le password da un luogo all'altro.
- Gli utenti non possono scrivere un processo di CA Process Automation che affermi che process.v = process.Password, perché v è visibile.
- Cambiamenti, come ad esempio l'aggiunta di una lettera "t" a una password e il successivo spostamento della "t", sono disabilitati durante l'utilizzo di JavaScript.
- Gli utenti non possono concatenare le password con un operatore +. Non sono autorizzate azioni che rivelino la password.
- Gli utenti non possono consentire il rilevamento dei contenuti delle password. Ad esempio, non possono rendere le parti nascoste visualizzabili.

In breve, CA Process Automation è di ausilio nel garantire la privacy della password finché questa opera all'interno di CA Process Automation. Le password che fanno parte delle configurazioni della categoria operatore sono protette. Non possono essere modificate o prese come riferimento o essere passate a metodi esterni.

Quando una password che non fa parte di una configurazione della categoria operatore viene passata a un metodo esterno, può essere restituita come testo non crittografato. Prendere precauzioni per proteggere le password che vengono passate a programmi esterni. L'ideale è utilizzare certificati o soluzioni alternative.

È possibile esportare i contenuti delle definizioni memorizzati in un database e quindi importarli in un database all'interno dello stesso dominio o in un dominio differente. L'importazione del set di dati in un altro dominio azzera le password poiché sono crittografate. Questo comportamento è per progettazione; domini differenti utilizzano chiavi di crittografia diverse.

## Informazioni sul certificato di CA Process Automation

Cercare le differenze tra l'utilizzo di un certificato autofirmato e di un certificato SSL attendibile in base alle proprie esigenze di protezione per CA Process Automation.

CA Process Automation fornisce un certificato autofirmato preconfigurato per l'utilizzo. È possibile gestire il certificato di CA Process Automation in uno dei seguenti modi:

- Usare il certificato fornito con CA Process Automation. Installare questo certificato da ogni browser da cui è possibile accedere all'URL dell'orchestrator di dominio di CA Process Automation.
- Creare un certificato autofirmato con l'apposita utility, crittografare la password con l'apposita utility, aggiornare il file delle proprietà con la posizione del keystore, password crittografata e alias del keystore.
- Ottenere un certificato da un'autorità di certificazione riconosciuta. Aggiornare il file delle proprietà con la posizione di keystore, password crittografata e alias del keystore.

**Importante.** Non rimuovere il keystore predefinito o il certificato autofirmato fornito con CA Process Automation. Questo certificato è necessario anche quando si configura CA Process Automation per utilizzare il proprio certificato autofirmato o un certificato ottenuto da un'autorità di certificazione (CA).

## Installare il certificato predefinito CA Process Automation

Se si accede a CA Process Automation con un URL che utilizza il protocollo HTTPS, il browser richiede un certificato rilasciato da un'autorità di certificazione (CA). Se si utilizza un certificato autofirmato CA Technologies quando si avvia CA Process Automation, il browser visualizza un avviso per informare che il certificato non è considerato attendibile.

**Per installare il certificato predefinito per CA Process Automation**

1. Aprire un browser, immettere l'URL per CA Process Automation, quindi accedere.
2. Se viene visualizzato un avviso di protezione, fare clic su Visualizza certificato.
3. Fare clic su Installa certificato e fare clic su OK.
4. Completamento della Creazione guidata.

   La prossima volta che si accede, non viene visualizzato un avviso di protezione.

## Informazioni sulla creazione di un certificato autofirmato

È possibile sostituire il certificato autofirmato fornito con CA Process Automation. Il certificato predefinito è configurato nel file OasisConfig.properties. Quando si crea un certificato autofirmato, il file di proprietà ed eseguire un file batch per firmare i file Jar (o archivio Java).

Prima di creare il proprio certificato, pianificare i valori per il percorso e l'alias keystore. Immettere i valori quando si esegue il keytool e quando si aggiorna il file di proprietà.

Utilizzare i seguenti file e utilità per implementare i certificati autofirmati:

- Utilità keytool

  **Nota:** per informazioni dettagliate su questa utility Java Sun cercare lo strumento di gestione chiavi - Strumento di gestione certificati e chiavi.

- PasswordEncryption.bat
- SignC2OJars.bat
- File OasisConfig.properties, in particolare, i seguenti tre parametri
  - itpam.web.keystorepath=

    **Predefinito:**

    *install_dir*/server/c2o/.config/c2okeystore

    **Nota:** il valore predefinito è il percorso del keystore autofirmato,

  - itpam.web.keystore.password=

    Il valore predefinito punta a domainID crittografato. Eseguire il file PasswordEncryption.bat quindi immettere la password keystore. Il programma batch genera la password crittografata nella console, che si specifica qui come nuovo valore.

  - itpam.web.keystorealias=

    **Impostazione predefinita**: ITPAM

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

## Creazione e implementazione del certificato autofirmato personale

È possibile creare un certificato autofirmato per sostituire il certificato autofirmato fornito con CA Process Automation.

**Attenersi alla procedura seguente:**

1. Utilizzando le credenziali di amministratore, accedere all'host in cui è installato l'orchestrator di destinazione.
2. Interrompere l'orchestrator (a pagina 196).
3. Se si intende riutilizzare il nome alias corrente per il keystore, rimuovere l'alias prima di continuare.
4. Eseguire il seguente comando per generare un keystore con lo strumento Java, Keytool. Specificare i valori per aliasname e per keystore_name. Il valore predefinito per aliasname è ITPAM. Se non si specifica un percorso per keystore, viene utilizzato il percorso corrente.

   ```
   keytool -genkey -alias "aliasname" -keyalg RSA -keystore
   "keystore_path.keystore"
   ```

   Ad esempio, accettare il percorso del keystore predefinito e immettere:

   ```
   keytool -genkey -alias "PAM" -keyalg RSA
   ```

   Vengono visualizzate le richieste di immissione e conferma della password keystore.

5. Immettere per entrambe le richieste la stessa password keystore. (Annotare la password per l'immissione successiva nell'utilità di crittografia).

   Viene visualizzata una serie di istruzioni seguita da un messaggio di conferma.

6. Rispondere ai messaggi con le informazioni richieste come segue:
   a. Immettere il nome e il cognome.
   b. Immettere il nome dell'unità aziendale.
   c. Immettere il nome dell'azienda.
   d. Immettere la città.
   e. Immettere la provincia.
   f. Immettere il codice paese a due cifre dell'unità organizzativa.

   Viene visualizzata una finestra di conferma delle voci nel formato, CN =valore, OU =valore, O =valore, L =valore, ST =valore, C =valore corretto?

7. Esaminare le voci e, se corrette, immettere Sì. Se le voci non sono corrette, immettere No e rispondere nuovamente alle richieste.
8. Rispondere ai prompt sulla password chiave per *aliasname* come descritto di seguito. L'opzione consigliata consente di evitare di immettere la password del certificato poiché ogni JAR viene firmato nel passaggio 13.
   - Immettere una password univoca per *aliasname*.
   - (Scelta consigliata) Premere Invio per utilizzare la password keystore come password alias.

   Un nuovo keystore viene creato nella directory corrente.
9. (Facoltativo) Consente di spostare il keystore in un altro percorso.
10. Crittografare la password keystore immessa nel passaggio 5.
    a. Modificare le directory nella directory *install_dir*/server/c2o.
    b. Eseguire PasswordEncryption.bat.
    c. Immettere la password keystore in risposta alla richiesta.

    L'utilità consente di crittografare la password keystore immessa e salvare i risultati nella console.
11. Eseguire il backup del file OasisConfig.properties. (*install_dir*/server/c2o/.config/OasisConfig.properties)
12. Aggiornare il file OasisConfiguration.properties come segue:
    a. Per itpam.web.keystorepath=, immettere il percorso assoluto al keystore, utilizzando "/" invece di "\", ad esempio, C:/*keystore_path*/keystore.
    b. Per itpam.web.keystore.password =, copiare e incollare la password keystore crittografata generata nel passaggio 9.
    c. Per itpam.web.keystore.alias =, immettere il nome alias specificato nel comando keytool nel passaggio 4.
13. Eseguire SignC2OJars.bat per firmare il JARS.

    Questo passaggio è necessario dopo l'aggiornamento del certificato o del keystore.
14. Avviare l'orchestrator (a pagina 197).

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

## Informazioni sull'utilizzo di certificato emesso da un'autorità di certificazione di terze parti

CA Process Automation supporta certificati di protezione di terzi per accesso Web HTTPS e firma di jars. Utilizzare le proprie risorse per ottenere un certificato SSL attendibile da un'autorità di certificazione di propria scelta. Questa procedura esula dall'ambito di questa guida.

L'uso di certificati di protezione di terze parti richiede l'uso di strumenti di terze parti. Il processo di installazione richiede inoltre modifiche manuali ai file di proprietà OasisConfig (*install_dir*/server/c2o/.config/OasisConfig.properties). Prima di iniziare, acquisire dimestichezza con le nozioni di base dei certificati di protezione e keystore e con l'utilità keytool fornita con Java JDK.

L'implementazione di certificati di protezione di terzi richiede l'aggiornamento dei valori per tre parametri nel file delle proprietà OasisConfig:

- "itpam.web.keystorepath"

  Il valore predefinito è il percorso del keystore per il certificato autofirmato:

  `install_dir/server/c2o/.config/c2okeystore`

- "itpam.web.keystore.password"

  Il valore predefinito è "domainID" crittografato.

- "itpam.web.keystorealias"

  Il valore predefinito è ITPAM.

  **Nota:** un keystore può disporre di più di un alias. Per utilizzare un alias del keystore che duplica un alias esistente, rimuovere l'alias esistente prima di aggiungere una nuova istanza.

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

## Implementazione del certificato SSL attendibile di terze parti

CA Process Automation supporta certificati di protezione di terzi per accesso Web HTTPS e firma di jars. È possibile ottenere tali certificati da un'autorità di certificazione di terze parti.

**Attenersi alla procedura seguente:**

1. Scegliere un password del certificato e ottenere un certificato di protezione da un'autorità di certificazione.
2. Utilizzando le istruzioni fornite dall'autorità di certificazione, importare il certificato in un keystore.

   In genere si utilizza un comando simile allo strumento di gestione chiavi –importa –alias *myalias* –file certfile –keystore "path_and_file_specification_for_keystore".
3. Per la password del keystore, immettere la password del certificato fornito dall'autorità di certificazione.
4. Ottenere una versione crittografata della password del keystore.
   a. Accedere a *install_dir*/server/c2o.
   b. Individuare lo script PasswordEncryption (PasswordEncryption.bat per Windows, PasswordEncryption.sh per UNIX o Linux).
   c. Eseguire PasswordEncryption passwordtoencrypt.
   d. Salvare il valore crittografato long restituito per voce nel file delle proprietà.
5. Interrompere l'orchestrator (a pagina 196).
6. Eseguire il backup e modificare il file delle proprietà di configurazione Oasis per aggiungere o aggiornare quanto segue:
   a. itpam.web.keystorepath per la posizione del keystore utilizzando il percorso completo e il nome del file per il file keystore.
   b. itpam.web.keystore.password con la password keystore crittografata (non racchiudere la password crittografata tra virgolette)
   c. Itpam.web.keystorealias per l'alias utilizzato per fare riferimento al certificato nel keystore (myalias negli esempi).
7. Firmare i file JAR eseguendo SignC2OJars (SignC2OJars.bat per Windows, SignC2OJars.sh per UNIX o Linux) incluso con CA Process Automation in *install_dir*/server/c2o. Eseguire SignC2oJars senza parametri per firmare il jars. Se la password del keystore immessa non corrisponde alla password del certificato, immettere la password del certificato quando vengono firmati i jar.

   **Nota**: su AIX si verifica un problema noto quando si firma per una seconda volta un file .jar utilizzando SignC2OJars. Per risolvere questo problema, annullare manualmente la firma dei file .jar tramite la rimozione dei file *.SF e *.RSA nella cartella META-INF per ogni archivio Java prima dell'esecuzione di SignC2OJars.

8. Se il keystore contiene più di un alias, modificare la voce del connettore server.xml. Il server.xm. è posizionato in <install_dir>\server\c2o\deploy\jbossweb-tomcat55.sar\server.xml. Aggiungere la riga in grassetto:

```
<Connector port="${tomcat.secure.port}"
address="${jboss.bind.address}"
   maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
   emptySessionPath="true"
   scheme="https" secure="true" clientAuth="false"
   keystoreFile="${itpam.web.keystorepath}"
   keyAlias="${itpam.web.keystorealias}"
   keystorePass="${itpam.web.keystore.password}" sslProtocol =
   "${SSL_PROTOCOL}" algorithm = "${X509_ALGORITHM}"
   useBodyEncodingForURI="true"/>
```

9. Avviare l'orchestrator (a pagina 197).
10. Ripetere questa procedura per ogni orchestrator in procinto di utilizzare il nuovo certificato.

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

# Gestione del nome host DNS

È possibile modificare il nome host per un orchestrator. Ad esempio, se il nome host non è conforme alla sintassi supportata, è possibile aggiornarlo. Se è stata eseguita l'installazione di CA Process Automation mediante un nome host DNS non valido, contenente caratteri limitati, come il carattere di sottolineatura, creare un alias conforme agli standard DNS. Quindi, sostituire manualmente il nome host non valido con questo alias nel proprio file OasisConfig.properties.

**Attenersi alla procedura seguente:**

1. Creare un alias. Consultare Abilitazione di DNS per risolvere un nome host non valido.
2. Accedere come amministratore al server in cui l'orchestrator di dominio è installato.
3. Accedere alla seguente cartella, dove install_dir indica il percorso in cui è installato l'orchestrator di dominio:

   `install_dir/server/c2o/.config`
4. Aprire il file OasisConfig.properties con un editor.
5. Utilizzare Trova per localizzare la proprietà seguente:

   `oasis.local.hostname`
6. Modificare il valore per la proprietà oasis.local.hostname=.
7. Salvare il file e uscire.
8. Riavviare il servizio Orchestrator.
   a. Interrompere l'orchestrator (a pagina 196).
   b. Avviare l'orchestrator (a pagina 197).

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

# Sintassi per nomi host del DNS

Vi sono numerosi percorsi in cui è possibile immettere un FQDN o un indirizzo IP. Se i nomi host del DNS includono un carattere di sottolineatura o non sono conformi alla sintassi richiesta, specificare l'indirizzo IP.

Nomi host del DNS validi:

- Inizia con una lettera.
- Finisce con un carattere alfanumerico.
- Contiene 2-24 caratteri alfanumerici.
- Può contenere il carattere speciale (-), segno di meno.

  **Importante.** Il segno di meno (-) è l'unico carattere speciale valido consentito nei nomi host del DNS.

# Disattivare i servizi Process Automation di Catalyst

I servizi Process Automation di Catalyst sono abilitati per impostazione predefinita. È possibile disabilitarli modificando un valore di proprietà nel file OasisConfig.properties.

**Attenersi alla procedura seguente:**

1. Accedere come amministratore al server in cui l'orchestrator di domino è installato.
2. Interrompere l'orchestrator (a pagina 196).
3. Accedere alla seguente cartella:

   `install_dir/server/c2o/.config`
4. Aprire il file OasisConfig.properties.
5. Scorrere fino al connettore integrato UCF nella sezione jboss-service.xml del file OasisConfig.properties.
6. Modificare il valore ucf.connector.enabled con false. Ad esempio:

   `ucf.connector.enabled=false`
7. Salvare il file e uscire.
8. Avviare l'orchestrator (a pagina 197).

**Ulteriori informazioni:**

File di proprietà di configurazione Oasis (a pagina 411)

# Appendice C: Introduzione di riferimento a OasisConfig.Properties

Questa sezione contiene il seguente argomenti:



I file di testo OasisConfig.properties controlla CA Process Automation. Le selezioni effettuate con il programma di installazione durante l'installazione dell'orchestrator di dominio, i relativi prerequisiti e oggetti vengono archiviati come valori di parametro nel file OasisConfig.properties.

**Importante.** Consentire l'aggiornamento del file OasisConfig.properties solo a un amministratore fidato.

La guida include gli argomenti seguenti sull'aggiornamento del file OasisConfig.properties:

- Controllo delle cache per gli aggiornamenti di CA EEM (a pagina 78).
- Modifica della porta di ascolto trap SNMP (a pagina 336).
- Configurazione delle proprietà di dominio (a pagina 147).
- Controllo del timeout per CA Process Automation (a pagina 20).
- Creazione e implementazione del certificato utente per CA Process Automation (a pagina 401).
- Disabilitazione dei servizi Process Automation di Catalyst (a pagina 407).
- Implementazione del certificato SSL attendibile di terze parti per CA Process Automation (a pagina 404).
- Gestione del nome host DNS (a pagina 406).
- Gestione degli indirizzi IP (a pagina 393).
- Impostazione del numero massimo di utenti e gruppi di CA EEM (a pagina 62).

La *Guida all'installazione* comprende gli argomenti seguenti sull'aggiornamento del file OasisConfig.properties:

- Abilitazione della disconnessione in CA Process Automation per SSO
- Abilitazione dell'autenticazione pass-through NTLM dopo l'installazione
- Generazione di file di certificato SSL
- Gestione del nome host DNS
- Prerequisiti di pianificazione delle porte
- Risoluzione del conflitto sulla porta per un agente

La *Guida di riferimento per la progettazione dei contenuti* comprende l'argomento seguente sull'aggiornamento del file OasisConfig.properties:

- Porte operatore

La *Guida di riferimento per i servizi Web* comprende gli argomenti seguenti sull'aggiornamento del file OasisConfig.properties:

- Comunicazioni
- executePendingInteraction

# File di proprietà di configurazione Oasis

Il file delle proprietà di configurazione Oasis (OasisConfig.properties) contiene le impostazioni di proprietà per ogni aspetto di CA Process Automation. Il file viene si trova nella cartella *install_dir*/server/c2o/.config. Tutti gli utenti con l'accesso al percorso di installazione di CA Process Automation possono modificare i file. Valutare di limitare l'accesso a questo percorso. Alcuni valori *non* devono essere modificati.

Le impostazioni includono:

**USE_DEPRECATED_COMMS_V1**

(Solo per gli agenti) Determina durante l'avvio di un agente se esso utilizza la modalità di comunicazione nuova o obsoleta. Si tratta di un valore boleano.

Quando la casella di controllo Usa comunicazione non più in uso è selezionata, questo valore è impostato su True. CA Process Automation:

- Termina la connessione con socket Web dell'agente, quindi passa tali informazioni a tutti gli orchestrator prima della conclusione.
- Svuota la mappa del server in cui sono archiviati questi dettagli sulla connessione.

Quando la casella di controllo Usa comunicazione non più in uso non è selezionata, questo valore è impostato su False.

- L'agente crea una nuova onnessione con socket Web e invia i dettagli sulla connessione per l'orchestrator.
- L'orchestrator salva i dettagli sulla connessione in una mappa del server.

Per ulteriori informazioni, consultare Determinazione della modalità di comunicazione degli agenti (a pagina 221).

**DOMAINID**

Definisce l'ID univoco per il dominio.

**Esempio**

```
ac04f945-f08b-4308-aa9c-c3fd95964f4d
```

**CLUSTERNODEID**

Determina un nodo esclusivamente in un cluster.

**Esempio**

```
8d11558a-3bf7-43d9-b394-4c055229e9ae
```

**KEYSTOREID**

Definisce la password keystore.

**Esempio**

```
ac04f945-f08b-4308-aa9c-c3fd95964f4d
```

**itpam.web.keystorepath**

Definisce il percorso keystore utilizzato per la firma dei file jar.

**Esempio**

```
C:/Program
Files/CA/PAMcert_Java7_Node2/server/c2o/.config/c2okeystore
```

**itpam.web.keystore.password**

Definisce la password keystore utilizzata per la firma dei file jar.

**Esempio**

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZLQotQj5
5Y8dPGRRXkrF4yTyk/IwzTcT0rLY+pWeGrGHaRKnlcXHL3fr7pYIzjVhoGd
rnRxSO4Prl70rIxqs3fCGIgFVIAnOzICQ9ct4qXIBIPnxQcgflrF0WDdaIj
CS6ubKwe9Wxhn0xjnmctvkLnMC1L74b48yQd9yhWSMAgpLAPLPJiMz/VoIz
cFVylqLS44KdM+wH6b6xkqVJECSH1GolBG2QUj/2
```

**itpam.web.keystorealias**

Definisce il nome di alias del certificato nel keystore utilizzato per la firma dei file jar.

**Esempio**

```
ITPAM
```

**CERTPASSWORD**

Definisce la password utilizzata per controllare l'accesso al keystore per la crittografia delle password e altri dati critici.

**Esempio**

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZXNASLuj
iOdl6POYm8CwjBTHnFUlbXQLcPqd+xc7oJkPF5X3cq8UHbEYL4iH+01b1Em
wHhw9uPXqDABcJqIJ+ECmODDAMn7rytSWqli+oxKp+e5scp1fnHjF1ENCKZ
NasYy6nF6vPozT9qLmB7DhzuFAvg8Av9J/U4ngYrZ5AMdU1sFP5Ddf3nw==
```

**oasis.database.username**

Definisce il nome utente per il server database della libreria.

**Esempio**

```
sa
```

**oasis.database.password**

Definisce la password associata all'utente del server database della libreria specificato.

**Esempio**

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZSSb28pT
xSL4fxuv+8IV8zLz+S6jwleU4mpQTDTM1xmwQ037qmAjDO74Y569W3LIP0v
BUEkJ30raf3/RsodMLdL3L51cnz8Gus4mJfGJla7WdTtzx0ts0BuUFPxZ1p
OpHOUUljFHn73243Iv7/pXIQe+O8lrHB00XotDicrleXavs+8sXSIPqKyX3
gmjy6LUZ
```

**oasis.database.dbhostname**

Definisce il nome host per il server database della libreria.

**Esempio**

```
lodivsa205
```

**oasis.database.dbport**

Definisce il numero di porta della connessione al server database della libreria.

**Esempio**

```
1433
```

**oasis.database.connectionurl**

Definisce l'URL di connessione JDBC al database della libreria.

**Esempio**

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

**oasis.database.databasetype**

Definisce il tipo di database della libreria.

**Esempio**

```
MSSQLServer2005
```

**oasis.database.dialect**

Definisce la classe di sottolinguaggio definita dall'utente del database della libreria.

**Esempio**

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

**oasis.database.genericdialect**

Definisce la classe di sottolinguaggio del database della libreria.

**Esempio**

```
org.hibernate.dialect.SQLServerDialect
```

**oasis.database.driver**

Definisce il nome completo della classe di driver JDBC.

**Esempio**

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

**oasis.database.typemapping**

Definisce il tipo di mapping per la sorgente dei dati.

**Esempio**

```
MS SQLSERVER2000
```

**oasis.database.exceptionsorter**

Definisce una classe che implementa l'interfaccia org.jboss.resource.adapter.jdbc.ExceptionSorter. L'interfaccia esamina le eccezioni di database per determinare se indicano un errore di connessione.

**Esempio**

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

**oasis.database.validConnectionChecker**

Definisce una classe che implementa l'interfaccia org.jboss.resource.adapter.jdbc.ValidConnectionChecker. L'interfaccia fornisce una modalità SQLException isValidConnection(Connection e). L'applicazione richiama la modalità con una connessione restituita dal pool per verificarne la validità.

**Esempio**

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConn
ectionChecker
```

**oasis.database.datasource.class**

Definisce la classe della sorgente dei dati.

**Esempio**

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

**oasis.database.additionalparamurl**

Definisce i parametri utilizzati per creare la connessione di database.

**Esempio**

```
responseBuffering=full;SelectMethod=cursor;
```

**oasis.database.lib.dbname**

Definisce il nome del database della libreria.

**Esempio**

```
pamgacert_cluster_JDK7_rep
```

**oasis.database.queues.dbname**

Definisce il nome del database delle code.

**Esempio**

```
pamgacert_cluster_JDK7_run
```

**oasis.reporting.database.databasetype**

Definisce il tipo di database di reporting.

**Esempio**

```
MSSQLServer2005
```

**oasis.reporting.database.username**

Definisce il nome utente per il server database di reporting.

**Esempio**

```
sa
```

**oasis.reporting.database.password**

Definisce la password associata all'utente specificato per il server database di reporting.

**Esempio**

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZoIzz9oH
5OU4XRkOaeLblNqEYDsaXNGiMg9LSy2P7gsVLG0ea32nBlUIvXgEXhiKfGz
IbCmYFgYoFg0sVBlnY/k1sAeZ21z20sw5Yr9HC2B3+IRoyy5LXCmByMUMc7
Ywq/BocPnw4e1DBDDfGqCQL/6ciK4CT1C7hU/V3Y4Ktrc9IsPK1aXeNRM1q
vpVwBAtG
```

**oasis.reporting.database.dbhostname**

Definisce il nome host per il server database di reporting.

**Esempio**

```
lodivsa205
```

**oasis.reporting.database.dbport**

Definisce il numero di porta della connessione al server database di reporting.

**Esempio**

```
1433
```

**oasis.reporting.database.genericdialect**

Definisce la classe di sottolinguaggio del database di reporting.

**Esempio**

```
org.hibernate.dialect.SQLServerDialect
```

**oasis.reporting.database.driver**

Definisce il nome completo della classe di driver JDBC.

**Esempio**

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

**oasis.reporting.database.typemapping**

Definisce il tipo di mapping per la sorgente dei dati.

**Esempio**

```
MS SQLSERVER2000
```

**oasis.reporting.database.dialect**

Definisce la classe di sottolinguaggio definita dall'utente del database di reporting.

**Esempio**

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

**oasis.reporting.database.ValidConnectionQuery**

Definisce un'istruzione SQL da eseguire su una connessione prima che sia restituita dal pool per verificarne la validità nel test delle connessioni obsolete del pool. Ad esempio: select count(*) from x.

**Esempio**

```
select 1
```

**oasis.reporting.database.connectionurl**

Definisce l'URL di connessione JDBC al database di reporting.

**Esempio**

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

**oasis.reporting.database.additionalparamurl**

Definisce i parametri aggiuntivi da utilizzare per creare la connessione al database.

**Esempio**

```
;responseBuffering=full;SelectMethod=cursor;
```

**FIPS_COMPLIANT**

Specifica se il server di CA Process Automation è conforme allo standard FIPS.

**Esempio**

```
true
```

**oasis.reporting.database.dbname**

Definisce il nome del database di reporting.

**Esempio**

```
pamgacert_cluster_JDK7_rpt
```

**oasis.runtime.database.dbtype**

Definisce il tipo di database di runtime.

**Esempio**

```
MSSQLServer2005
```

**oasis.runtime.database.username**

Definisce il nome utente per il server database di runtime.

**Esempio**

```
sa
```

**oasis.runtime.database.password**

Definisce la password associata all'utente specificato per il server database di runtime.

**Esempio**

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZSOIjQ79
jp66tm5E7ZYxLV2yqtVV54HRVs+xvNksG7p1pzTZOoOXahwS0XOcVoMl8Mz
nkgQgVOllCIU/YBx6lT3ZAxnzOMY2xBQnIp5xTxw0Dv5eqqTvpOnm6P2vPO
S1RzYGA6GRt3VdASiTZwZs/BkIX/sY+6C52V/x5Eg7l4hff6/6gS6wvRHdJ
G/sXU6D6
```

**oasis.rntime.database.dbhostname**

Definisce il nome host per il server database di runtime.

**Esempio**

```
lodivsa205
```

**oasis.runtime.database.port**

Definisce il numero di porta della connessione al server database di runtime.

**Esempio**

```
1433
```

**oasis.runtime.database.dialect**

Definisce la classe di sottolinguaggio definita dall'utente del database di runtime.

**Esempio**

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

**oasis.runtime.database.genericdialect**

Definisce la classe di sottolinguaggio del database di runtime.

**Esempio**

```
org.hibernate.dialect.SQLServerDialect
```

**oasis.runtime.database.driver**

Definisce il nome completo della classe di driver JDBC.

**Esempio**

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

**oasis.runtime.database.typemapping**

Definisce il tipo di mapping per la sorgente dei dati.

**Esempio**

```
MS SQLSERVER2000
```

**oasis.runtime.database.exceptionsorter**

Definisce una classe che implementa l'interfaccia org.jboss.resource.adapter.jdbc.ExceptionSorter per esaminare le eccezioni di database in modo da determinare se l'eccezione indica un errore di connessione.

**Esempio**

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

**oasis.runtime.database.ValidConnectionQuery**

Definisce un'istruzione SQL da eseguire su una connessione prima che sia restituita dal pool per verificarne la validità nel test delle connessioni obsolete del pool. Ad esempio: select count(*) from x.

**Esempio**

```
select 1
```

**oasis.runtime.database.validConnectionChecker**

Definisce una classe che implementa l'interfaccia di org.jboss.resource.adapter.jdbc.ValidConnectionChecker per fornire un metodo SQLException isValidConnection(Connection e). Una connessione restituita dal pool richiama questo metodo per verificarne la validità.

**Esempio**

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConn
ectionChecker
```

**oasis.runtime.database.datasource.class**

Definisce la classe della sorgente dei dati.

**Esempio**

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

**oasis.runtime.properties.table.create.stmt**

Definisce l'istruzione SQL da utilizzare per creare la tabella delle proprietà se non è presente. Non è prevista alcuna modifica dall'utente per questa istruzione, in quanto l'applicazione configura per impostazione predefinita il valore corretto per il database pertinente.

**Esempio**

```
create table properties (propkey varchar(255) NOT
NULL,propvalue NVARCHAR(MAX),PRIMARY KEY (propkey))
```

**oasis.runtime.database.connectionurl**

Definisce l'URL di connessione JDBC al database di runtime.

**Esempio**

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

**oasis.runtime.database.additionalparamurl**

Definisce i parametri aggiuntivi utilizzati per creare la connessione di database.

**Esempio**

`;responseBuffering=full;SelectMethod=cursor;`

**oasis.runtime.database.driver.name**

Definisce il nome di driver del database di runtime.

**Esempio**

`com.microsoft.sqlserver.jdbc.SQLServerDriver (per un database MSSQL)`

**oasis.runtime.database.dbname**

Definisce il nome del database di runtime.

**Esempio**

`pamgacert_cluster_JDK7_run`

**oasis.security.server.type**

Definisce il tipo di server di protezione utilizzato per l'autenticazione e l'autorizzazione.

**Esempio**

`EEM`

**oasis.policy.type**

Definisce il tipo di policy di accesso.

**Esempio**

`EEM`

**certificatefolderFullpath**

Definisce il percorso della cartella contenente il certificato di protezione. Il percorso è relativo alla cartella c2o.

**Esempio**

*install_dir*`/server/c2o/.c2orepository/public/certification/`

**oasis.eem.backend.server.location**

Definisce il nome host del computer che ospita il server di protezione EEM.

**Esempio**

`lodivsa205`

**oasis.eem.application.name**

Definisce il nome dell'applicazione nel server EEM su cui vengono definite le policy per l'istanza corrente di CA Process Automation.

**Esempio**

`pamgacert_cluster_JDK7`

**isFipsMode**

Specifica se il server EEM è in esecuzione in modalità FIPS.

**Esempio**

```
false
```

**oasis.eem.certificate.path**

Indica il nome del certificato di protezione.

**Esempio**

```
PAM.p12
```

**eiamCertKeyPath**

Definisce il nome del file di chiave per il certificato di protezione utilizzato per l'autenticazione. Questa proprietà è applicabile solo se isFipsMode=true.

**Esempio**

```
PAM.key
```

**oasis.eem.certificate.password**

Definisce la password associata al certificato di protezione EEM. Questa proprietà è applicabile solo se isFipsMode=false.

**Esempio**

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZdD65vFT
Vmbn8aaZxjot9QCUIfPEey1H8/KGtNShgrronJk0rMtqliDMrNo2VE+xoAU
DcfmT9IPCQsAe497w1xUBkHg8PbZNjWVkPpFYw496eFiwiq7AoyB8WCoUrx
8wVnkMjoGs1BqDND+kjHcnUt9HLljYgxatT7Q2FpbTA7+Qag0W9gSv2oH4i
BsUjVs22
```

**ntlm.enabled**

Specifica se è abilitata l'autenticazione NTLM. Durante la modifica di questa porta, rimuovere la cartella .c2o dalla cartella ${Installation Dir}/server/c2o/.system, se presente.

**oasis.jxta.port**

Definisce la porta da utilizzare per la comunicazione con altri orchestrator o agenti.

**Esempio**

```
7001
```

**oasis.jxta.host**

Definisce il nome host del computer utilizzato per la comunicazione con l'orchestrator o l'agente.

**Esempio**

*name*`03-I40136.ca.com`

**oasis.local.hostname**

Definisce il nome host del computer in cui è installato CA Process Automation.

**Esempio**

*name*03-I40136.ca.com

**oasis.server.isCluster**

Specifica se di questa istanza di CA Process Automation è inclusa in un cluster.

**Esempio**

true

**loadbalancer.worker.node**

Definisce il nome di questo nodo nel cluster. Questa proprietà è applicabile solo se compresa in un cluster.

**Esempio**

node2

**oasis.snmptrigger.service.port**

Definisce la porta di ascolto per trigger SNMP.

**Esempio**

162

**oasis.transport.secure**

Specifica se la comunicazione è protetta.

**Esempio**

true

**AcceptAllSSLCertificates**

Specifica se accettare tutti i certificati in comunicazione protetta.

**Esempio**

true

**oasis.reject.unnecessary.approval**

Specifica se rifiutare un modulo di interazione che non è stato configurato per l'approvazione.

**Esempio**

true

**managementconsole.timeout**

Definisce il timeout (in minuti) per CA Process Automation. Il timeout corrisponde all'intervallo di inattività di CA Process Automation, trascorso il quale la sessione scade.

**Esempio**

30

**eem.connection.retries**

Definisce il numero di nuovi tentativi per l'autenticazione quando il server di protezione è EEM.

**Esempio**

```
3
```

**SSL_PROTOCOL**

Definisce il tipo di protocollo SSL. Se il vendor Java è IBM Corporation, viene utilizzato il protocollo SSL. Negli altri casi viene utilizzato l'algoritmo TLS.

**Esempio**

```
TLS
```

**X509_ALGORITHM**

Definisce l'algoritmo utilizzato per i certificati SSL. Se il vendor Java è IBM Corporation, l'algoritmo utilizzato è IbmX509. Negli altri casi viene utilizzato l'algoritmo SunX509.

**Esempio**

```
SunX509
```

**oasis.publisher.name**

Definisce il nome con cui questa istanza di CA Process Automation viene concessa in licenza.

**Esempio**

```
CA
```

**jboss.partition.udpgroup**

Definisce l'indirizzo multicast per questo nodo cluster.

**Esempio**

```
228.1.46.192
```

**jboss.rmi.port**

Definisce la porta del servizio di denominazione RMI.

**Esempio**

```
1098
```

**jboss.jndi.port**

Definisce la porta di ascolto per il servizio JNP del bootstrap (JNDI Provider).

**Esempio**

```
1099
```

**jboss.rmi.classloader.webservice.port**

Definisce la porta utilizzata per il servizio HTTP semplice che supporta richieste per classi per il carico di classe dinamica RMI, org.jboss.web.WebService.

**Esempio**

```
8083
```

**jboss.rmi.object.port**

Definisce la porta di ascolto per il socket del server RMI a cui i client RMI si connettono durante la comunicazione tramite l'interfaccia proxy.

**Esempio**

```
4444
```

**jboss.pooledinvoker.serverbind.port**

Definisce la porta di binding per il server dell'invoker in pool.

**Esempio**

```
4445
```

**remoting.transport.connector.port**

Definisce la porta di binding per il server remoto.

**Esempio**

```
4448
```

**jboss.ha.jndi.port**

Definisce la porta su cui lo stub HA-JNDI viene reso disponibile.

**Esempio**

```
1100
```

**jboss.ha.jndi.rmi.port**

Definisce la porta RMI utilizzata dal servizio HA-JNDI in caso di binding.

**Esempio**

```
1101
```

**jboss.ha.rmi.object.port**

Definisce la porta di oggetto RMI utilizzata da JRMPInvokerHA.

**Esempio**

```
4447
```

**jboss.ha.pooledinvoker.serverbind.port**

Definisce la porta di binding per il server HA dell'invoker in pool.

**Esempio**

```
4446
```

**jboss.mcast.jndi.autodiscovery.port**

Definisce la porta di gruppo multicast utilizzata per l'individuazione automatica di JNDI. Questa porta viene definita nei file cluster-service.xml e hajndi-jms-ds.xml in deploy/jms.

**Esempio**

`1102`

**jboss.mcast.ha.partition.port**

Specifica la porta UDP multicast per HAPartition. Questa porta viene definita nei file n cluster-service.xml e jmx-console.war/WEB-INF/web.xml.

**Esempio**

`45566`

**jboss.mcast.http.sessionreplication.port**

Specifica la porta UDP multicast per la replica HttpSession. Questa porta viene definita nel file tc5-cluster-service.xml.

**Esempio**

`45567`

**tomcat.connector.http.port**

Definisce la porta per il componente di connettore che supporta il protocollo HTTP/1.1. Questa proprietà consente a Catalina di funzionare come un server Web autonomo, oltre alla possibilità di eseguire servlet e pagine JSP. La porta è configurata anche in jboss-ws4ee.sar/META-INF/jboss-service.xml per Axis Service.

**Esempio**

`8080`

**tomcat.connector.ajp.port**

Definisce la porta per il componente di connettore che comunica con un connettore Web mediante il protocollo AJP.

**Esempio**

`8009`

**tomcat.secure.port**

Definisce la porta protetta utilizzata dal connettore SSL. Questa porta non è utilizzata. Questa è la stessa porta configurata come

- redirectPort per il connettore AJP in server.xml
- WebServiceSecurePort per Axis Service in jboss-ws4ee.sar/META-INF/jboss-service.xml

La porta viene utilizzata solo se il connettore SSL è abilitato.

**Esempio**

`8443`

**jboss.uil.serverbind.port**

Definisce la porta a cui i client del servizio UIL (Unified Invocation Layer) si connettono quando stabiliscono una connessione con il server JBossMQ.

**Esempio**

```
8093
```

**oasis.protection.level**

Specifica il livello di protezione di CA Process Automation. In modalità protetta, il livello di protezione è impostato su RISERVATO, altrimenti è impostato su NESSUNO.

**Valori:** NESSUNO, INTEGRALE o RISERVATO.

**itpam.initialperiodicheartbeatfrequency**

Definisce la frequenza di heartbeat iniziale (in minuti).

**Esempio**

```
2
```

**system.encoding**

Definisce la codifica di questo sistema.

**Esempio**

```
Cp1252
```

**eem.max.search.size**

Definisce il numero massimo di record da cercare contemporaneamente in EEM.

**Esempio**

```
10000
```

**jboss.remoting.transport.Connector.port**

Definisce una porta correlata a JBoss.

**Esempio**

```
3873
```

**OAPort**

Definisce una porta correlata a JBoss.

**Esempio**

```
3528
```

**OASSLPort**

Definisce una porta correlata a JBoss.

**Esempio**

```
3529
```

**scripts.tmpDir**

Definisce il valore della directory temporanea che esegue gli script.

**Esempio:**

```
C:/Users/ADMINI~1/AppData/Local/Temp/2
```

**oasis.powershell.setexecutionpolicy**

Specifica se l'utente ha selezionato un'opzione per modificare la policy di esecuzione di PowerShell durante l'installazione.

**Esempio**

```
false
```

**oasis.powershell.path**

Definisce il percorso di PowerShell sul computer host.

**Esempio**

```
C:/Windows/System32/WindowsPowerShell/v1.0
```

**override.jvm.tmpdir**

Specifica se sostituire la variabile di sistema java.io.tmpdir. Il valore predefinito (true) consente al server di rinviare la variabile di sistema a c2oHome/tmp. Impostare questa proprietà su false se non si desidera che il server rinvii la variabile di sistema a c2oHome/tmp.

**Esempio**

```
true
```

**jboss.default.jgroups.stack**

Definisce il tipo di stack predefinito impostato per l'utilizzo da JGroups ai fini dell'esecuzione dell'applicazione.

**Esempio**

```
tcp
```

**jboss.jgroups.tcp.tcp_port**

Definisce la porta TCP per il clustering basato sul protocollo TCP in JBoss.

**Esempio**

```
7600
```

**jboss.jgroups.tcp_sync.tcp_port**

Definisce la porta di sincronizzazione TCP per il clustering basato sul protocollo TCP in JBoss.

**Esempio**

```
7650
```

**jboss.messaging.datachanneltcpport**

Definisce la porta di un canale dati per messaggistica basata sul protocollo TCP.

**Esempio**

`7900`

**jboss.messaging.controlchanneltcpport**

Definisce la porta di un canale comandi per messaggistica basata sul protocollo TCP.

**Esempio**

`7901`

**jts.default.tx.reaper.timeout**

Definisce un numero intero non negativo richiesto da JBoss Transaction Service.

**Esempio**

`120000`

**jboss.transaction.timeout**

Definisce l'ora in cui il reaper avvia il timeout delle transazioni in corso in seguito alla scadenza di un timeout. Questa proprietà è obbligatoria per JBoss.

**Esempio**

`300`

**jboss.service.binding.port**

Definisce il file Ref deploy/messaging/remoting-bisocket-service.xml. Questa proprietà è obbligatoria per JBoss Messaging.

**Esempio**

`4457`

**jboss.remoting.port**

Definisce il file Ref deploy/jmx-remoting.sar. Questa proprietà è obbligatoria per JBoss Remoting.

**Esempio**

`1090`

**jboss.jbm2.port**

Definisce il trasporto di comunicazione a JBoss Messaging. Questa proprietà è obbligatoria per JBoss Messaging 2 Netty.

**Esempio**

`5445`

**jboss.hbm2.netty.ssl.port**

JBoss. Questa proprietà è obbligatoria per la versione SSL di Netty.

**Esempio**

`5446`

**jboss.tx.recovery.manager.port**

Definisce il file Ref deploy/transaction-jboss-beans.xml. Questa proprietà è obbligatoria per JBossTS Recovery Manager.

**Esempio**

`4712`

**jboss.tx.status.manager**

Definisce il file Ref deploy/transaction-jboss-beans.xml. Questa proprietà è obbligatoria per JBossTS Transaction Status Manager.

**Esempio**

`4713`

**jboss.tx.manager.sock.pid.port**

Definisce il file Ref deploy/transaction-jboss-beans.xml. Questa proprietà è obbligatoria per JBossTS.

**Esempio**

`4714`

**ucf.payload.file**

Definisce il nome del file che contiene il payload del contenitore Catalyst.

**Esempio**

`catalyst.installer.payload.zip`

**catalyst.container.name**

Definisce il nome del contenitore Catalyst.

**Esempio**

`node0`

**ucf.connector.enabled**

Specifica se i servizi Process Automation di Catalyst sono abilitati.

**Esempio**

`false`

**ucf.payload.override**

Specifica se sovrascrivere il payload (se presente).

**Esempio**

`false`

**ucf.pax.web.http.port**

Definisce la porta /container/etc/org.ops4j.pax.web.cfg.

**Esempio**

`8181`

**ucf.bus.hostname**

Definisce il nome host del bus Catalyst in /registry/topology/physical/node0/catalyst-bus/bus.properties.

**Esempio**

```
hostlocale
```

**ucf.bus.port**

Definisce la porta del bus Catalyst in /registry/topology/physical/node0/catalyst-bus/bus.properties.

**Esempio**

```
61616
```

**ucf.bus.http.port**

Definisce la porta HTTP del bus Catalyst in /registry/topology/physical/node0/catalyst-bus/bus.properties.

**Esempio**

```
61617
```

**ucf.max.archive.query.results**

Definisce i risultati per la query di massima archiviazione.

**Esempio**

```
30
```

**use.catalyst.claims.credentials**

Specifica se utilizzare le attestazioni Catalyst per le credenziali.

**Esempio**

```
false
```

**org.apache.commons.logging.Log**

Definisce una classe factory per istanziare i logger per Commons Logging.

**Esempio**

```
org.apache.commons.logging.impl.Log4JLogger
```

**org.apache.commons.logging.LogFactory**

Definisce una classe factory per istanziare i logger per Commons Logging.

**Esempio**

```
org.apache.commons.logging.impl.Log4jFactory
```

**eem.cache.timeout**

Questo parametro aggiunto dall'utente definisce la validità massima, espressa in secondi, della cache per l'archiviazione delle credenziali utente con il profilo di autorizzazioni associato. Se impostato su zero, la cache per l'autorizzazione di CA Process Automation viene disattivata e CA Process Automation invia una richiesta a CA EEM ogni volta che sono necessarie le autorizzazioni utente. Quando questo parametro manca, CA Process Automation utilizza una frequenza di aggiornamento di 30 secondi per la cache secondaria.

**Nota:** Per informazioni sulle due cache di CA EEM, consultare la sezione Controllo della frequenza di aggiornamento per la cache degli aggiornamenti di CA EEM (a pagina 78).

**Esempio**

30

**mail.attachment.buffer.size**

Consente di scaricare un messaggio di posta elettronica con un valore di buffer specificato.

K è l'unità di misura. Ad esempio, se si specifica 256, CA Process Automation lo definisce come 256 KB.

**Esempio**

mail.attachment.buffer.size=256

**mail.imap.fetchsize**

Questa proprietà è specifica del protocollo IMAP e non è introdotta per CA Process Automation. Questa proprietà consente di scaricare più velocemente allegati di posta elettronica di grandi dimensioni.

Specificare questa proprietà in byte.

**Esempio**

Per specificare 800 KB, moltiplicare 800*1024.

mail.imap.fetchsize=819200